Software Engineering Institute

Pattern-Based Design of Insider Threat Programs

Andrew P. Moore
Matthew L. Collins
David A. Mundie
Robin M. Ruefle
David M. McIntire

December 2014

TECHNICAL NOTE
CMU/SEI-2014-TN-024

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon University

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001852

Table of Contents

List of Figures

Abstract

Despite the high impact of insider attacks, organizations struggle to implement effective insider threat programs. In addition to the mandate for all Department of Defense (DOD) and U.S. Government agencies to build such programs, approval of updates to the *National Industrial Security Program Operating Manual* regarding insider threat defense require thousands of contractors to have insider threat programs as part of their security defense. Unfortunately, according to the Insider Threat Task Force of the Intelligence and National Security Alliance (INSA) Cyber Council, many such organizations have no insider threat program in place, and most of the organizations that do have serious deficiencies. This report describes a pattern-based approach to designing insider threat programs that could, if further developed, provide a more systematic, targeted way of improving insider threat defense.

1 Introduction

The understanding of insider threat in the CERT® Division of the Software Engineering Institute stems from a decade of cataloging more than 800 cases of *malicious insider* crime against information systems and assets, including more than 120 cases of espionage involving classified national security information. Our research has revealed that malicious insiders exploit business process vulnerabilities as often as they exploit technical vulnerabilities. Likewise, our data analysis has identified more than 100 categories of weaknesses in enterprise architectures that have allowed insider attacks to occur. We used this analysis to develop an assessment method for insider threat vulnerability that is based on qualitative models of insider information technology (IT) sabotage and insider theft of intellectual property (IP). These models characterize patterns of malicious or suspicious insider behaviors seen in insider threat cases.

An organizational pattern "addresses the structure of a development organization and describes a commonly recurring structure of interacting human or departmental roles that solves a development process problem" [Buschmann 2007]. *Enterprise architecture patterns* are organizational patterns that involve the full scope of enterprise architecture concerns, including people, processes, technology, and facilities [Klein 2010]. The broad scope of enterprise architecture patterns allows us to describe an insider's authorized access—both online and physical—to organizational systems.

In addition to defining patterns from models of insider IT sabotage and insider theft of IP, we also applied these models to develop best practices and technical controls for mitigating insider threat. In some cases of insider threat, departing insiders might take valuable IP with them. One set of practices and controls designed to reduce the risk of insider IP theft is based on case data showing that 70% of insider IP thieves stole at least some IP 60 days or fewer before their termination, whether forced or voluntary. The pattern describing this set of practices and controls helps to balance the costs of monitoring employee behavior for suspicious actions against the risk of losing the organization's IP [Moore 2012, 2011].

Organizations aware of this pattern can ensure that they have the necessary agreements in place with employees (IP ownership and consent to monitoring), identify critical IP, monitor departing insiders, and communicate necessary information among departments. When an insider resigns or is fired, the organization increases its technical monitoring and scrutiny of that employee's activities within a 60-day window of the termination date. Organizations must take action at the time of and before an employee's termination to ensure their IP is not compromised and to preserve their legal options.

This report discusses an insider threat mitigation pattern language that can be used by organizations to develop their insider threat capability along various dimensions. We describe the pattern language and discuss three capability development scenarios, or paths through the pattern language, that organizations can use to develop insider threat mitigation capabilities.

2 A Preliminary Insider Threat Mitigation Pattern Language

Describing our understanding of insider threat mitigations as architectural pattern languages provides effective solutions to the insider threat problem in a clear format for organizations. In the software engineering community, a pattern language is “a network of interrelated patterns that define a process for resolving software development problems systematically” [Buschmann 2007]. Pattern languages are necessary to guide developers from one pattern application to another.

The *Related Patterns* section of each subject pattern identifies patterns in the language that can be applied after the subject pattern is applied to further the mitigation approach. The *Context* section of the subject pattern describes the conditions under which the pattern can be applied. The structure that results is a directed network of patterns—the pattern language. Figure 1depicts a preliminary language for insider threat mitigation that addresses several concerns related to insider theft and sabotage.

The patterns in show five pattern groups that can help organizations understand the enterprise, get the right workforce in place, create the right culture within the workforce, manage the employees within the workforce, and cut ties with the employee when appropriate (whether voluntarily on the part of the employee or not). The groupings are shown as nested since, in general, the patterns in groupings to the top and left must be applied before patterns in groupings to the bottom and right (e.g., an organization must get the workforce in place before it can create the right culture within that workforce). The grouping on top, *Understanding the Enterprise*, provides patterns that help to determine the security needs of the organization, the risks to its critical assets, and a strategy for improving its insider threat capabilities. The four groupings below the top one were chosen to reflect the workforce employment lifecycle. The *Appendix B* provides a thumbnail sketch of the patterns in these four groupings. *Appendix A* provides a simple ontology for the domain covered by the patterns.

The elaboration of the insider threat mitigation language is a work in progress. Additional groupings may be added or existing groupings refined as the language continues to grow. Our previous work has identified patterns important to insider threat mitigation based on the wealth of insider threat case data collected by the CERT Division [Mundie 2012]. We have come to view this previous work as a *pattern collection* rather than a pattern language. This pattern collection is a source we can use to mine patterns for the future refinement of the pattern language described in this report. This report, therefore, provides a blueprint for our future efforts.

The directed graph in Figure 1, shown as pattern names connected by blue arrows, documents the mitigation pattern language structure. Patterns at the target of an arrow refine patterns at the source (i.e., the target pattern occurs in the *Related Patterns* section of the source pattern). Patterns at the bottom of one grouping (except the last) are implicitly connected to patterns at the top of the next grouping. Other patterns in a grouping may be linked to a pattern in a later grouping, but those links are explicitly designated (e.g., the link from *Log Employee Actions* to *Handle Employee Departure)*. Cycles are possible when a pattern can lead to the re-application of a previously applied pattern, as shown in the bottom of the third grouping. Future work will elaborate these patterns in a format commonly accepted by the patterns community.

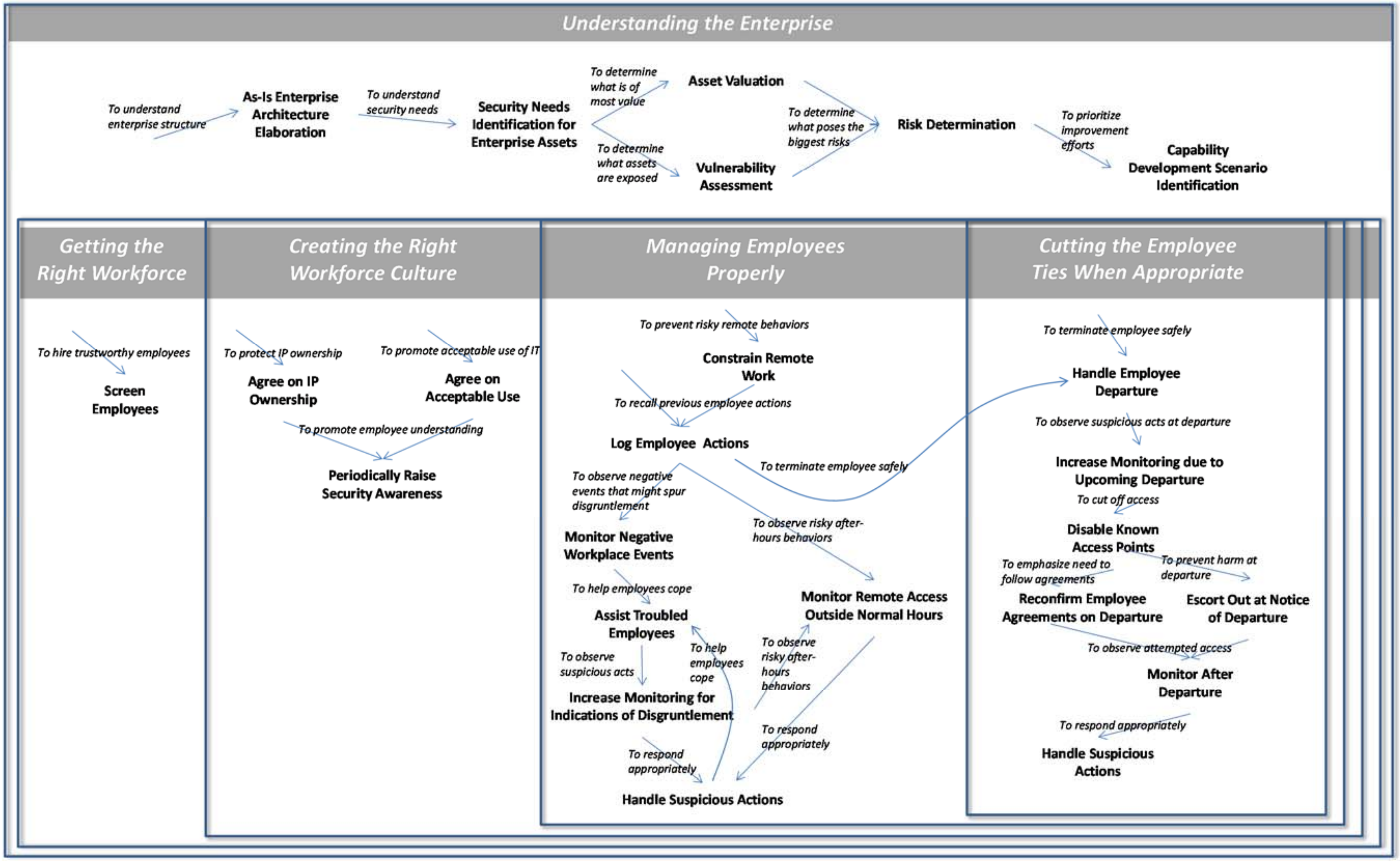
Understanding the Enterprise
To understand enterprise structure
As-Is Enterprise Architecture Elaboration
To understand security needs
Security Needs Identification for Enterprise Assets
To determine what is of most value
Asset Valuation
To determine what assets are exposed
Vulnerability Assessment
To determine what poses the biggest risks
Risk Determination
To prioritize improvement efforts
Capability Development Scenario Identification
Getting the Right Workforce
To hire trustworthy employees
Screen Employees
Creating the Right Workforce Culture
To protect IP ownership
Agree on IP Ownership
To promote acceptable use of IT
Agree on Acceptable Use
To promote employee understanding
Periodically Raise Security Awareness
Managing Employees Properly
To prevent risky remote behaviors
Constrain Remote Work
To recall previous employee actions
Log Employee Actions
To terminate employee safely
To observe negative events that might spur disgruntlement
Monitor Negative Workplace Events
To observe risky after-hours behaviors
Monitor Remote Access Outside Normal Hours
To help employees cope
Assist Troubled Employees
To observe suspicious acts
To help employees cope
To observe risky after-hours behaviors
Increase Monitoring for Indications of Disgruntlement
To respond appropriately
To respond appropriately
Handle Suspicious Actions
Cutting the Employee Ties When Appropriate
To terminate employee safely
Handle Employee Departure
To observe suspicious acts at departure
Increase Monitoring due to Upcoming Departure
To cut off access
Disable Known Access Points
To emphasize need to follow agreements
To prevent harm at departure
Reconfirm Employee Agreements on Departure
Escort Out at Notice of Departure
To observe attempted access
Monitor After Departure
To respond appropriately
Handle Suspicious Actions

Figure 1: Preliminary Insider Threat Mitigation Pattern Language

Arrows in Figure 1 are labeled with a description of the goal associated with applying the pattern at the arrow target. So, for example, *to hire trustworthy employees*, you apply the *Screen Employees* pattern. Once applied, you decide whether it is more important for you *to protect IP ownership* or *to promote acceptable use of IT*, and apply the respective pattern in each case. Paths through the pattern language, generally from top to bottom within a grouping and left to right from one grouping to another, improve an organization's capability to mitigate the insider threat along some specific dimension.

Patterns in the pattern languages higher in the graph along a path (including those in groupings to the left) must be applied before patterns that are lower along the same path. The pattern language does not specify the ordering of adjacent patterns (i.e., patterns along two different paths). A simple example is that the organization can institute agreements on IP ownership and acceptable use in either order as far as the pattern language is concerned.

While mitigation along a specific dimension might be accomplished by following a specific path from top to bottom and left to right, more comprehensive mitigation can be achieved by following multiple paths, or by traversing the directed graph more completely. Of course, these patterns are not likely to be applied from scratch—fundamental business processes and organizational structures are likely to already be in place. Higher level patterns that have been, in effect, applied in the organization's as-is enterprise architecture can either be skipped or used to fine-tune the enterprise architecture based on the guidance provided by the pattern. In this way, an organization can use the language to improve its current enterprise architecture, rather than starting from scratch.

3 Using the Insider Threat Mitigation Pattern Language

As described in the 2005 article, *Sequences as a Basis for Pattern Language Composition*, pattern languages are more about structure than about temporal sequence [Porter 2005]. In contrast, pattern sequences emphasize the temporal structure of patterns. In the context of our insider threat mitigation pattern language, we refer to important pattern sequences as *capability development scenarios (CDSs)*. These scenarios are identified by the *Capability Development Scenario Identification* pattern in the *Understanding the Enterprise* grouping.

A CDS designates a path through the mitigation pattern language—specifically the four employee lifecycle groupings—with the goal of mitigating a specific insider threat behavior. Figure 2 designates three CDSs. The name of each CDS represents its associated goal: *Mitigating Telework Abuse* (shown in orange), *Mitigating Disgruntlement at Negative Workplace Events* (shown in purple), and *Mitigating Theft of IP at Departure* (shown in green).

- ***Mitigating Telework Abuse:*** Analysis of insider threat cases with relevant data shows that over half of the cases of insider IT sabotage involved remote access outside the insider's normal working hours [Flynn 2013]. This CDS involves making sure honest candidates are hired and that these candidates understand what constitutes acceptable use of the organization's IT systems. The organization decides what remote access employees are allowed to have based on their job function, the resources accessed, and the time and day of the access. Certain remote access may be denied and other remote access audit logs may be monitored closely. Suspicious access will be handled via explicitly defined policy.
- ***Mitigating Disgruntlement at Negative Workplace Events:*** Analysis of insider threat cases with relevant data shows that 57% of the cases of insider IT sabotage involved an attack within 60 days of the insider's termination from the organization [Flynn 2013]. While it was not shown that the termination was the cause of attack, it does suggest that employee actions around their termination should be monitored closely for suspicious behavior. Other types of negative workplace events seen in sabotage cases include being passed over for promotion, being demoted, and being denied financial bonuses to which employees had become accustomed. This CDS follows a path through the pattern language that starts similar to the *Mitigating Telework Abuse* CDS as shown in Figure 2. Keeping audit logs of employee actions enables monitoring of employees for signs of disgruntlement around negative workplace events. The organization's response due to suspicious employee actions depends on the severity of those actions. Severe malicious behaviors may warrant the insider's termination. Less egregious behaviors may warrant referral to employee assistance programs, albeit with potentially closer monitoring of employee actions.

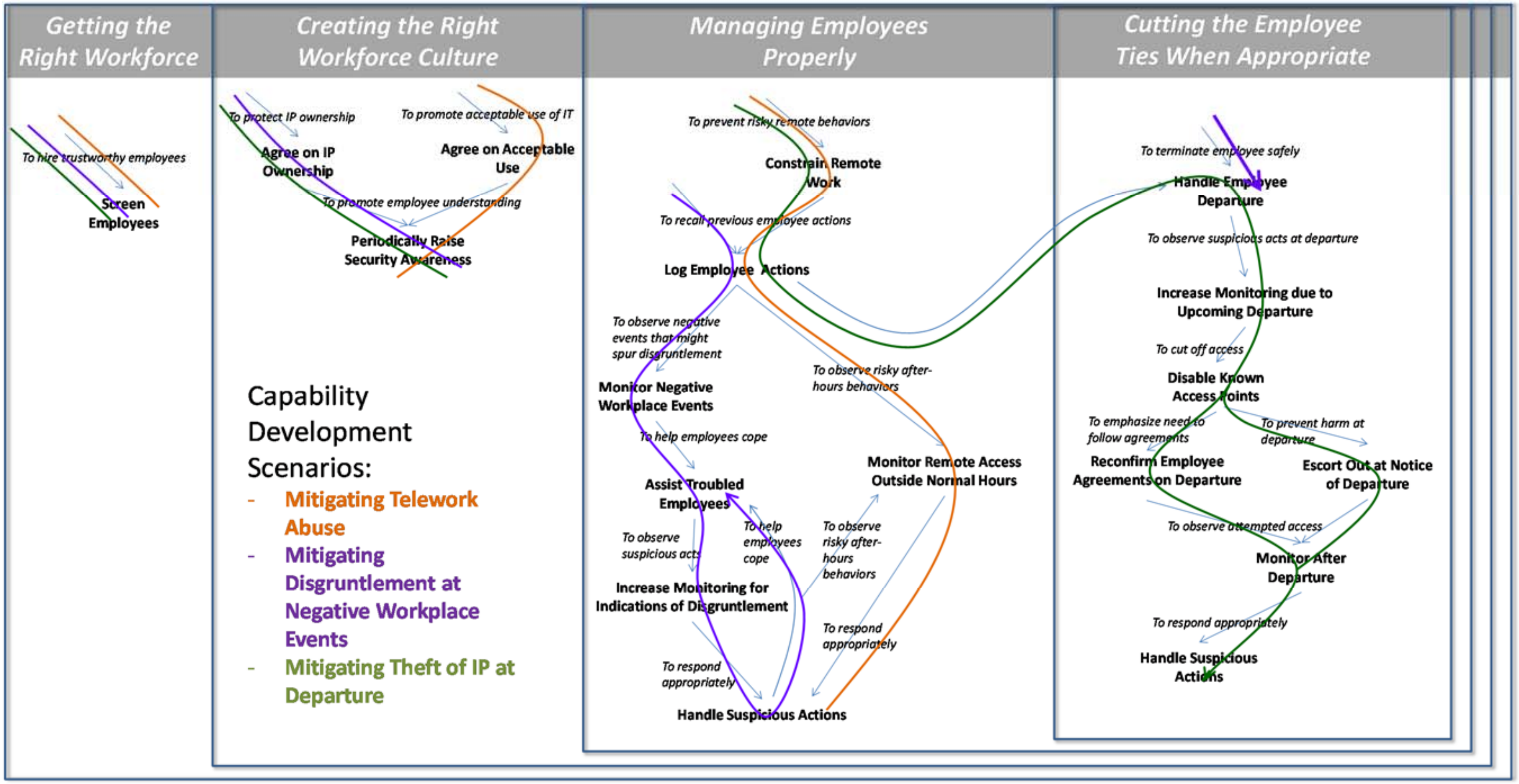
Getting the Right Workforce
Creating the Right Workforce Culture
Managing Employees Properly
Cutting the Employee Ties When Appropriate
To hire trustworthy employees
Screen Employees
To protect IP ownership
To promote acceptable use of IT
Agree on IP Ownership
Agree on Acceptable Use
To promote employee understanding
Periodically Raise Security Awareness
Capability Development Scenarios:
- Mitigating Telework Abuse
- Mitigating Disgruntlement at Negative Workplace Events
- Mitigating Theft of IP at Departure
To prevent risky remote behaviors
Constrain Remote Work
To recall previous employee actions
Log Employee Actions
To observe negative events that might spur disgruntlement
Monitor Negative Workplace Events
To observe risky after-hours behaviors
To help employees cope
Monitor Remote Access Outside Normal Hours
Assist Troubled Employees
To observe suspicious acts
To help employees cope
To observe risky after-hours behaviors
Increase Monitoring for Indications of Disgruntlement
To respond appropriately
To respond appropriately
Handle Suspicious Actions
To terminate employee safely
Handle Employee Departure
To observe suspicious acts at departure
Increase Monitoring due to Upcoming Departure
To cut off access
Disable Known Access Points
To emphasize need to follow agreements
To prevent harm at departure
Reconfirm Employee Agreements on Departure
Escort Out at Notice of Departure
To observe attempted access
Monitor After Departure
To respond appropriately
Handle Suspicious Actions

Figure 2: Capability Development Scenarios

- ***Mitigating Theft of IP at Departure:*** Similar to insider IT sabotage, analysis shows that 70% of insider IP thieves stole at least some intellectual property within 60 days of the insider's termination from the organization [Moore 2012]. Agreement on the ownership of IP must be made upon employee hiring. An insider's departure may be voluntary or forced. Insiders forced to leave are escorted out of the building with pay until the date of termination. Insiders who are voluntarily terminated are subject to increased monitoring for signs of IP exfiltration. In either case, the insider's access is disabled at termination and the insider's agreement on IP ownership is reviewed with the insider at his or her exit interview. Monitoring insider actions that occur 60 days prior to termination takes place and continues for 60 days after termination. Any suspicious behaviors, including the uncharacteristic download of IP, especially in large quantity, is dealt with according to the severity of the behavior, preferably with Human Resources or Legal personnel involvement.

CDSs can be elaborated as abstracted swimlane flowchart diagrams (in the terminology of Business Process Model and Notation [BPMN], but also known as interaction diagrams in Unified Modeling Language [UML]) as exemplified in Figure 3. The swimlane flowchart is abstracted in the sense that the diagram shows the interactions only *between* swimlanes rather than the detailed process flow within each swimlane. Finally, a more descriptive representation of a CDS is a pattern story, an example of which is provided below.

Pattern Story: Mitigating Theft of IP by Departing Insiders

Acme creates advanced products for catching quick-footed birds of various breeds. On a previous occasion, one of Acme's competitors developed a product that was suspiciously similar to a product that Acme had in the last stages of development but had not publicly announced. Worse yet, a short time prior to the competitor's release, the competitor hired a previous Acme employee who had knowledge of the product. Since the organization ***Audit Logs Employee Actions***, its records showed that the previous employee had downloaded the latest product software just prior to departure. Without ***Agreeing on IP Ownership***, the company had no effective recourse and lost significant market share among their wiliest customers since it was beaten to market.

Acme could not let this happen again and remain competitive in this looney tunes, cut-throat market. While Acme decided it could not ***Escort Out at Notice of Departure***, except in the case of acrimonious termination (because of lost productivity), they did decide that to ***Handle Employee Departure*** they could ***Increase Monitoring due to Upcoming Departure*** for the 60 days around the insider's termination as suggested by the CERT Division of the SEI. This approach would leverage the audit logs they had in place and focus the human-intensive monitoring tasks to the point of greatest vulnerability—the window of time around termination. After termination, Acme would ***Disable Known Access Points*** and ***Monitor after Departure*** the terminated insider's activities. Upon the discovery of suspicious acts, such as downloading large quantities of IP or exchanging uncharacteristic email with competitors, Acme would ***Handle Suspicious Actions***.

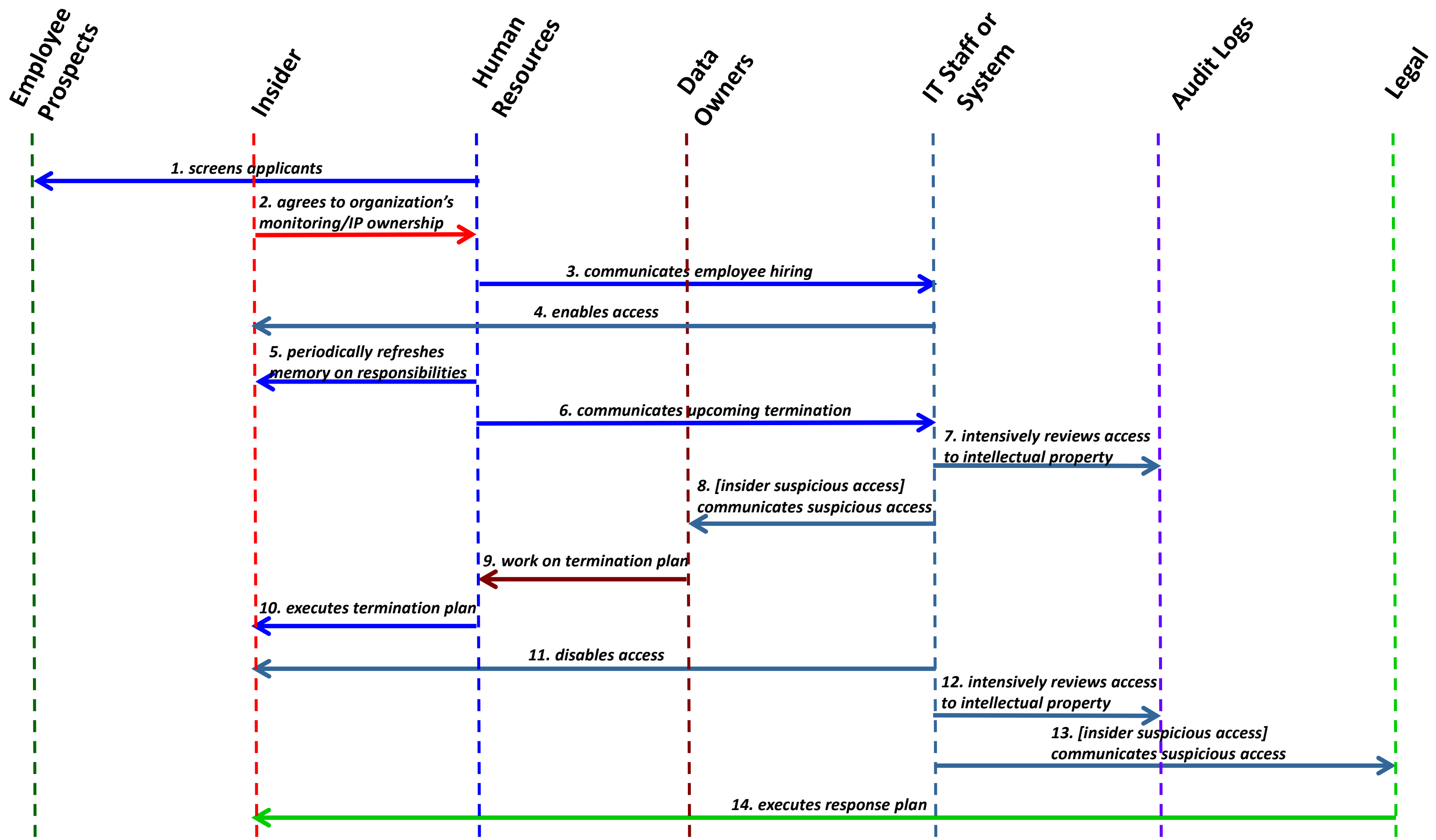
Employee Prospects
Insider
Human Resources
Data Owners
IT Staff or System
Audit Logs
Legal
1. screens applicants
2. agrees to organization's monitoring/IP ownership
3. communicates employee hiring
4. enables access
5. periodically refreshes memory on responsibilities
6. communicates upcoming termination
7. intensively reviews access to intellectual property
8. [insider suspicious access] communicates suspicious access
9. work on termination plan
10. executes termination plan
11. disables access
12. intensively reviews access to intellectual property
13. [insider suspicious access] communicates suspicious access
14. executes response plan

Figure 3: Abstracted Swimlane Diagram for the Mitigating Theft of IP by Departing Insiders CDS

Acme also decided to start to ***Screen Employees*** at hiring to minimize their exposure to candidates whose past experiences predispose them to stealing IP. To make sure insiders know their rights and responsibilities, Acme required insiders to ***Agree on IP Ownership*** with all employees at hiring, to ***Periodically Raise Security Awareness*** through formal training, and to ***Reconfirm Employee Agreements on Departure***.

Acme's strategy ultimately paid off. Since its implementation, they have not had any known incidents of insider theft of IP, have remained competitive in the bird-catching market, and have not alienated their staff with unnecessarily harsh or restrictive working conditions.

Sequence of Patterns in the CDS Story

1. Screen Employees
2. Agree on IP Ownership
3. Periodically Raise Security Awareness
4. Log Employee Actions
5. Handle Employee Departure
6. Increase Monitoring due to Upcoming Departure
7. Disable Known Access Points
8. Reconfirm Employee Agreements on Departure
9. Monitor After Departure
10. Handle Suspicious Actions

4 Conclusion

This report describes research to create and validate an insider threat mitigation pattern language that helps organizations prevent, detect, and respond to insider threats. The language is organized so that specific paths through the language can help organizations develop their insider threat capability along different dimensions. Continuing our efforts to help federal agencies and contractors develop insider threat programs per Executive Order 13587, we are now seeking active government partners to apply and refine our approach [White House 2011]. We also are continuing our research into fundamental patterns of insider threat mitigation to make sure that they remain well-grounded and validated scientifically.

Appendix A: Simple Insider Threat Mitigation Pattern Domain Ontology

Figure 4 depicts a simple insider threat mitigation domain ontology for the patterns outlined in this paper. The entity-relationship diagram shows key concepts referred to in patterns as boxes and the relationships between concepts as labeled arrows between the boxes.

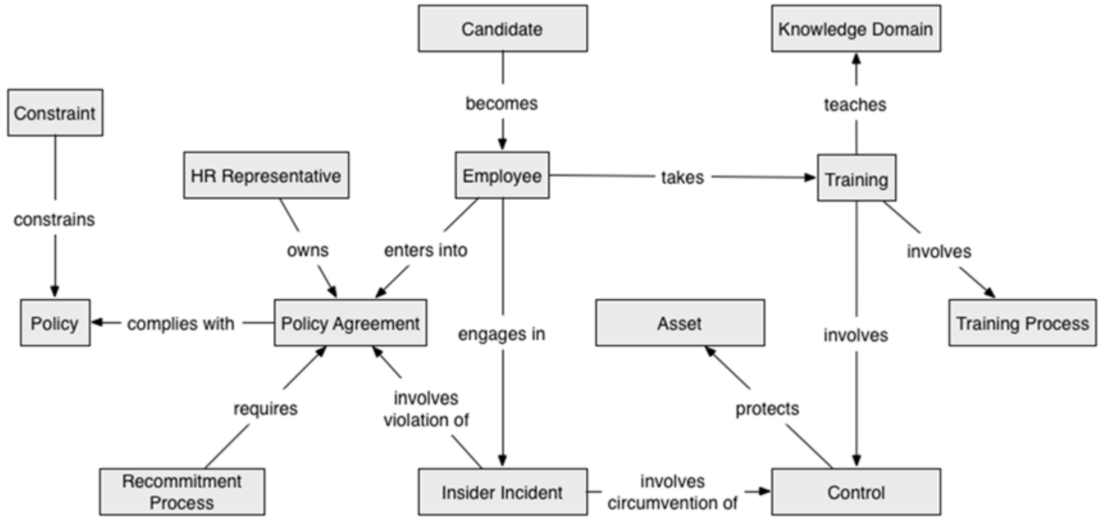

Figure 4: Insider Threat Mitigation Domain Ontology

As shown on the left side of the figure, *policies* have *constraints* and *policy agreements* must comply with *policies*. Types of constraints may include fairness, clarity, and enforceability. Policies that are relevant to insider threat involve intellectual property, telework, monitoring, security, acceptable use, employee termination, and incident management.

Policy agreements are an important mechanism for institutionalizing policies. As shown in the figure, the agreement involves an *HR representative* who explains the policy and is responsible for its enforcement, and an *employee*. In addition, the *recommitment process* periodically reminds the employee that he or she entered into the policy agreement. *Candidates* can become employees who then must take training.

Training involves a *training process* conducted to teach a *knowledge domain*. Some example knowledge domains include:

- Dealing with difficult employees
- Developing corporate culture
- Disgruntlement mitigation
- Employee assistance
- Employee termination
- Negative workplace events
- Positive intervention

Training can also include education on the purpose, configuration, and use of a *control* intended to prevent, detect, respond to, or otherwise mitigate a threat to an *asset*. An employee may engage in an *insider incident* which may involve the violation of a *policy agreement* and/or the circumvention of an organizational *control*.

Appendix B: Insider Threat Mitigation Pattern Thumbnail Sketches

1. Agree On Acceptable Use Policies

Context: An employee is using devices on his employer's network to perform his job.

Problem: Employees may exploit a real or false lack of knowledge about the acceptable use of devices on a network and engage in conduct that is counter to his employer's interests.

Solution: HR representatives of organizations should require employees to sign an acceptable use policy agreement before using devices connected to a network.

Related Patterns: Periodically Raise Security Awareness

2. Agree on Intellectual Property Ownership

Context: An employee is accessing information on his employer's network to perform his job.

Problem: Employees may be unaware of, or chose to ignore, the organization's ownership rights to information produced by employees of the organization, and, as a result, mishandle that information.

Solution: As a condition of employment, HR representatives of organizations should require employees to sign an intellectual property ownership policy agreement that specifies the rights that the organization has to any intellectual property to which the employee has access or develops.

Related Patterns: Periodically Raise Security Awareness

3. Assist Troubled Employees

Context: An employee is involved in a negative workplace event.

Problem: Troubled employees may have a higher likelihood of committing an insider incident.

Solution: Organizations can assist troubled employees in a way that provides them remediation and reduces their ill will toward the organization, thus avoiding an insider incident.

Related Patterns: Increase Monitoring for Indications of Disgruntlement

4. Constrain Remote Work

Context: An employee uses remote access to access the organizations information or systems purportedly to perform authorized functions.

Problem: Employees may exploit remote access to sabotage the organization's operations or to remove intellectual property in an unauthorized manner. [Flynn 2013]

Solution: Organizations should restrict remote access to an organization's network, either by restrictions to access timeframe (e.g., outside normal work hours) or restrictions to access relative to local network use, in a manner that enhances the organization's ability to protect itself and its assets.

Related Patterns: Log Employee Actions

5. Disable Known Access Points

Context: An employee is departing an organization for employment elsewhere and the organization has a comprehensive record of access paths the employee has for accessing the organization's systems.

Problem: Employees who depart an organization under problematic circumstances may become angry to the point of wanting to steal information from the organization or compromise the integrity of the organization's information or information systems. Active access paths into the organization's systems after departure provide the opportunity to do those things. [Flynn 2013]

Solution: Organizations should disable employee accounts that it knows about upon employee departure, and prepare to monitor suspicious remote access after departure for signs of unauthorized access attempts.

Related Patterns: Reconfirm Employee Agreements on Departure, Escort Out on Notice of Departure

6. Escort Out at Notice of Departure

Context: An employee resigns from his or her position within an organization.

Problem: Employees may attempt to exploit a flaw in organization security during the period between their notification of departure (or dismissal) and their exit from the premises.

Solution: The organization escorts the employee from the premises at the point of the employee's notification of departure or of the employee's dismissal.

Related Patterns: Monitor After Departure

7. Handle Employee Departure

Context: An employee has left or is preparing to leave an organization

Problem: Departing employees may be more willing to commit an insider incident due to the removal of dismissal or other disciplinary actions as a potential punishment.

Solution: The organization maintains usable, up-to-date policies on employee departure and trains managers in maintaining sympathetic but unyielding focus on the policies during the exit process.

Related Patterns: Increase Monitoring Due to Upcoming Departure

8. Handle Suspicious Actions

Context: An organization detects suspicious activity attributed to an employee

Problem: It is often difficult to distinguish employee actions that are a part of their normal job function and those that are counter to the organization's interest.

Solution: The organization investigates employee activity to decide whether suspicious activity warrants employee assistance, organizational sanctions, or - in the extreme of criminal conduct - employee termination and legal action.

Related Patterns: Assist Troubled Employees

9. Increase Monitoring Due to Upcoming Departure

Context: An employee is departing an organization voluntarily or not.

Problem: Employees preparing to depart an organization may be more likely to perpetrate an insider incident.

Solution: The organization should increase the monitoring of employees preparing to depart the organization. Previous analysis shows that organizations should consider analyzing employee transactions 60 days prior to the departure date, though smaller or larger monitoring windows may be desirable depending on the risk tolerance of the organization. [Moore 2012]

Related Patterns: Disable Known Access Points

10. Increase Monitoring for Indications of Disgruntlement

Context: An employee has displayed some indication that they are having troubles either personally or professionally.

Problem: Troubled employees may have a higher likelihood of committing an insider incident, even if the organization has tried to deal with the issue previously. [Flynn 2013]

Solution: Organizations should increase monitoring of disgruntled employees to determine whether an employee displays continued or increasing signs of disgruntlement.

Related Patterns: Handle Suspicious Actions

11. Log Employee Actions

Context: An employee is using devices on his employer's network to perform his job.

Problem: Organizations may not be able to attribute suspicious or malicious actions to the employee engaged in those actions.

Solution: Organizations should log routine employee actions that could be a component of a malicious act.

Related Patterns: Monitor Negative Workplace Events, Monitor Remote Access Outside Normal Hours, Handle Employee Departure

12. Monitor After Departure

Context: An employee is involved in a negative workplace event prior to or during their departure.

Problem: Employees may still wish to harm their employing organization even after their departure, possibly by using intellectual property gathered during employment or by using old access paths to harm the organization.

Solution: Organizations should monitor former employees and their potential online actions for signs that they may be trying to harm the organization.

Related Patterns: Handle Suspicious Actions

13. Monitor Negative Workplace Events

Context: An employee has agreed to and is trained on organization policies.

Problem: Negative workplace events may spur disgruntlement and be the motivation for an insider incident. [Flynn 2013]

Solution: Organizations should monitor negative workplace events that could be a precursor to or a component of an insider incident.

Related Patterns: Assist Troubled Employees

14. Monitor Remote Access Outside Working Hours

Context: An employee has authorized remote access to the organization's information and systems.

Problem: To evade detection, employees may exploit remote access outside of working hours to conduct activities that harm the organization.

Solution: Organizations should monitor remote access connections after working hours for suspicious activity. [Flynn 2013]

Related Patterns: Handle Suspicious Actions

15. Periodically Raise Security Awareness

Context: An employee using devices on a network is subject to constraints on their behavior to ensure security.

Problem: Employees may not recall or may feign not recalling a particular policy governing their behavior or controls for the protection of assets.

Solution: Organizations should train employees regarding their security responsibilities and compel them to periodically reaffirm their commitment to policies they have previously agreed to as part of that training.

Related Patterns: Constrain Remote Access, Log Employee Actions

16. Reconfirm Employee Agreements on Departure

Context: A departing employee has agreed to and is trained on organization policies.

Problem: Employees may either forget about previous policy agreements or feign ignorance of employment agreements making violations of those agreements more likely.

Solution: Organizations should discuss with departing employees their previous employee agreements and require them to recommit to those agreements before departure.

Related Patterns: Monitor After Departure

17. Screen Employees

Context: An individual (candidate) is attempting to gain employment at the organization.

Problem: Candidates may have participated in detectable prior incidents that make their employment inherently risky, or otherwise be unsuitable for the position at hand.

Solution: Organizations should perform background checks on candidates and hire only individuals who meet some minimum criteria for employment.

Related Patterns: Agree on IP Ownership, Agree on Acceptable Use Policies

References/Bibliography

URLs are valid as of the publication date of this document.

[Buschmann 2007]

Buschmann, F.; Henney, K.; & Schmidt, D. C. *Pattern-Oriented Software Architecture Volume 5: On Patterns and Pattern Languages.* Wiley, 2007.
http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471486485.html

[White House 2011]

The White House. *Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 2011. http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-

[Flynn 2013]

Flynn, Lori; Clark, Jason; Moore, Andrew, P.; Collins, Matthew; Tsamitis, Eleni; Mundie, David; & McIntire, David. “Four Insider IT Sabotage Mitigation Patterns and an Initial Effectiveness Analysis.” *Proceedings of the Conference on Programming Languages of Programs (PLOP).* Monticello: ACM, 2013.

[Hafiz 2011]

Hafiz, Munawar; Adamczyk, Paul; & Johnson, Ralph. "Growing a Pattern Language (for Security)." *Proc. of the Conference on Pattern Languages of Programs (PLOP).* Portland: ACM, 2011.

[Klein 2010]

Klein, John & Gagliardi, Michael. *A Workshop on Analysis and Evaluation of Enterprise Architectures.* (CMU/SEI-2010-TN-023), Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9363

[Moore 2012]

Moore, Andrew P.; McIntire, David; Mundie, David; & Zubrow, David. "Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders." *Proc. of the Conference on Pattern Languages of Programs (PLOP).* Albuquerque: ACM, 2012.

[Moore 2011]

Moore, Andrew P.; Hanley, Michael J.; & Mundie, David A. "A Pattern for Increased Intellectual Property Theft Monitoring of Departing Insiders." *Proc. of the Conference on Pattern Languages of Programs (PLoP).* Portland, OR: ACM, 2011.

[Mundie 2012]

Mundie, David A.; Moore, Andrew P.; & McIntire, David. "Building a Multidimensional Pattern Language for Insider Threats." *Proc. of the Conference on Pattern Languages of Programs (PLoP).* Albuquerque: ACM, 2012.

[Porter 2005]
Porter, Ronald; Coplien, James O.; & Winn, Tiffany. "Sequences as a Basis for Pattern Language Composition." *Science of Computer Programming, Special Issue on New Software Composition Concepts* 56 (2005): 231-249. http://dl.acm.org/citation.cfm?id=1072132

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE December 2014	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE
Pattern-Based Design of Insider Threat Programs

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Andrew P. Moore, Matthew L. Collins, David A. Mundie, Robin M. Ruefle, & David M. McIntire

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2014-TN-024

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFLCMC/PZE/Hanscom
Enterprise Acquisition Division
20 Schilling Circle
Building 1305
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Despite the high impact of insider attacks, organizations struggle to implement effective insider threat programs. In addition to the mandate for all Department of Defense (DOD) and U.S. Government agencies to build such programs, approval of updates to the *National Industrial Security Program Operating Manual* regarding insider threat defense require thousands of contractors to have insider threat programs as part of their security defense. Unfortunately, according to the Insider Threat Task Force of the Intelligence and National Security Alliance (INSA) Cyber Council, many such organizations have no insider threat program in place, and most of the organizations that do have serious deficiencies. This report describes a pattern-based approach to designing insider threat programs that could, if further developed, provide a more systematic, targeted way of improving insider threat defense.

14. SUBJECT TERMS
insider threat, patterns

15. NUMBER OF PAGES
25

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL