Four Insider IT Sabotage Mitigation Patterns and an Initial Effectiveness Analysis

LORI FLYNN, CERT® Division, Software Engineering Institute
JASON CLARK, CERT Division, Software Engineering Institute
ANDREW P. MOORE, CERT Division, Software Engineering Institute
MATTHEW COLLINS, CERT Division, Software Engineering Institute
ELENI TSAMITIS, CERT Division, Software Engineering Institute
DAVID MUNDIE, CERT Division, Software Engineering Institute
DAVID MCINTIRE, CERT Division, Software Engineering Institute

This paper describes four patterns of insider IT sabotage mitigation and initial results from an investigation of 46 relevant cases for pattern effectiveness. The four IT sabotage mitigation patterns are represented in the case data, suggesting that some cases might have been prevented, detected earlier, or responded to more effectively if the suggested solutions were implemented. To our knowledge, there has been no previous successful demonstration or attempted use of the patterns described in this paper. The initial effectiveness analysis shows supporting but inconclusive results due to insufficient (case and baseline) data.

1.1 INTRODUCTION

Insider information technology (IT) sabotage occurs when an insider uses IT to direct specific harm at an organization or an individual [11]. In this paper, we describe four mitigation patterns to prevent, detect, and effectively respond to insider IT sabotage:

1) Constrain Remote Work Outside of Normal Hours.
2) Increase Monitoring Within a Time Window of a Negative Workplace Event.
3) Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely.
4) Eliminate Potential Methods of Access After Termination.

In addition to the four mitigation patterns, we provide initial results from an analysis of 46 relevant cases performed to determine pattern effectiveness. For this paper, we define an *insider* as a current or former employee, contractor, or business partner. *Insider IT sabotage* is defined as malicious alteration, destruction, or deletion of IT systems or data (on IT systems) with potential or actual harm caused. Throughout this paper we define the risk of insider IT sabotage as the product of *Consequence x Vulnerability x Threat* [12]. Though we have not quantified the values of consequence, vulnerability, or threat, this definition of risk allows us to examine the underlying drivers of risk and to identify strategies to mitigate risk.

Common aspects of attacks are represented in case data as well as in the four insider IT sabotage mitigation patterns, suggesting that some cases might have been prevented, detected earlier, or responded to more effectively if the suggested solutions were implemented. While the data associated with the patterns exist, to our knowledge, there are no previous successful demonstrations or attempted uses of the four patterns described in this paper to mitigate the insider threat. Although there has been no known application of the four patterns described in this paper, "the process of pattern mining is similar to scientific discovery" and allows us to test our patterns as potential mitigation strategies [10]. We collected data from cases in the CERT® Insider Threat Center's MERIT

A preliminary version of this paper was presented in a writers' workshop at the 20th Conference on Pattern Languages of Programs (PLoP). PLoP'13, October 23-26, Monticello, Illinois, USA. Copyright 2013 is held by the author(s). HILLSIDE 978-1-941652-00-8

® CERT is a registered mark owned by Carnegie Mellon University. The CERT Division is part of the Software Engineering Institute, a U.S. Department of Defense federally-funded research and development center.

Database and conducted analyses to test our hypotheses that our patterns are effective strategies to mitigate insider threat.

1.2 Paper Order

This paper is ordered as it is for the following reasons: We describe the patterns in Section 2 to enable you to understand our pattern effectiveness analysis in relation to the patterns. Because our patterns are testable hypotheses, we collected data and performed analyses to demonstrate the patterns' potential effectiveness in practice. Section 3, "Initial Effectiveness Analysis," describes the methodology we used for testing and the analysis results for each pattern. Our effectiveness analysis consisted of analyzing cases in an insider threat IT sabotage case history database to test for pattern matches. We present the data we collected about the cost of our patterns in Section 4 to provide you with an understanding of the financial impact of implementing these patterns.

1.3 Pattern Format

This paper's pattern format, for the most part, is based on aspects deemed important in the book *Pattern-Oriented Software Architecture, On Patterns and Pattern Languages, vol. 5* [14], while recognizing that there are many possible pattern formats and that the book describes many different formats. The book includes an examination of the written form of patterns.

For clear communication and useful critique, the form must express the pattern unambiguously. The book authors call the following aspects *important* for characterizing a pattern: **name, context of the problem in which it arises, summary of the problem, forces that make up the problem, summary of the proposed solution, detailed elaboration of the solution, and discussion of consequences of introducing the solution**. (This type of form is sometimes called a POSA form.) Style is also discussed as important for clarity, so the use of formatting is relevant, including emphasis indicated by using bold text and bulleted lists of forces. The book argues that forces of personal aesthetics must be balanced against the technical message of the content and clear communication to the intended audience.

This paper describes four closely related patterns and uses a consistent pattern description form for each. Formalized sectioning, bulleted forces, indentation, and text bolding are all used for clarity. Our pattern descriptions include the aforementioned important pattern aspects in sections of our pattern format, and include additional aspect sections. The technical and policy-based problems our patterns address can be difficult to describe clearly and concisely without examples. Examples are suggested by Buschmann, Henney and Schmidt in their book *Pattern-Oriented Software Architecture, On Patterns and Pattern Languages, vol. 5* [14] because patterns are empirical in nature, although the book does not include examples in its list of *important* aspects of a written pattern.

The ***Example*** section describes a problem that happens without the pattern, and the ***Example Resolved*** section describes the same situation with the mitigating pattern (preventing, detecting, or helping effective response to) the problem.

The ***Design Rationale*** section explains why the pattern was developed. It first explains how the problem was identified using case data information, which is a common feature of our four patterns, but not common to many other types of patterns in the pattern community. Previous patterns have used similar case data analysis to identify problems [3, 4, 7]. In this section, we also explain why each proposed pattern might ameliorate the problem, since that it might not be quickly obvious.

Finally, we added the ***Other Relevant Patterns*** section, to show connections between the pattern and existing pattern-related work. Diagrams help you to quickly understand relationships that are difficult or lengthy to express in words, so we use the ***Diagram*** section to help convey meaning about the patterns.

Although some pattern formats use ratings to identify confidence in the pattern [15, 16], we did not include ratings because our analysis of effectiveness determined that we had too little data to draw conclusive results, despite the fact that our data did (weakly or insignificantly) support the pattern hypotheses.

1.4 Related Work

Over the last 10 years, the CERT Division of Carnegie Mellon University's Software Engineering Institute has coded and analyzed over 800 cases of malicious insider threats. This extensive and ongoing research of insider threats has determined that most cases exhibit a variety of patterns [8]. Our pattern development and analysis expands the CERT Division's existing body of pattern analysis, which itself is based on related patterns work.

Frank and Hohimer developed a predictive modeling approach to insider threat mitigation based on known patterns from the CERT Division [2]. Their predictive model aims to incorporate a diverse set of data sources that not only addresses the cyber domain, but also the physiological and motivational factors that may underlie malicious insider exploits. Frank and Hohimer define triggers in terms of observable cyber and psychosocial indicators and higher level aggregated patterns [2].

Based on initial modeling work and the analysis of CERT cases, Moore et al. found that different classes of insider crimes exhibit different patterns of problematic behavior and require different mitigation measures [3]. Specifically, this research introduces the concepts of "entitled independent" and "ambitious leader" as models of insider theft of intellectual property (IP). Moore et al. identified enterprise architectural patterns that protect against a variety of insider threats. The CERT Division's insider threat database reveals that over 50% of insider theft of IP happens within 30 days of insider termination [2].

Recent analysis provides a decision-making framework for organizations that want to reduce their risk of insider IP theft based on their unique exposure [7]. Mundie et al. developed 26 patterns for insider threat in their paper *Building a Multidimensional Pattern Language for Insider Threats*; the authors' main objective for the paper was to organize those patterns into a language using a multidimensional pattern language [5]. The patterns we identify in this paper expand on that work and will be incorporated into the Mundie et al. pattern language. The architectural patterns and subsequent pattern systems by Mundie et al. enable coherent reasoning about how to design and implement enterprise systems to protect against insider threat by understanding the patterns of insiders [4]. Similarly, the mitigation patterns we developed are designed to provide effective methods to prevent, detect, and respond to insider threats.

2. INSIDER IT SABOTAGE MITIGATION PATTERNS

The following sections describe four patterns we identified for mitigating insider IT sabotage. The format of the patterns is described in Section 1.3.

2.1 Pattern 1: *Constrain and Monitor Remote Work Outside of Normal Hours.*

Our case data indicate that many insiders who commit insider IT sabotage do so remotely, outside normal working hours (NWO). *Remote* refers to the insider being offsite from the organization when conducting the attack. If an insider logs in from home to launch an attack on the organization's system, that insider attacks remotely. *Outside normal hours* refers to a time beyond the insider's usual working hours (e.g., if the insider normally works 2PM-10PM, 9AM is outside normal hours).

Design Rationale. Remote access after normal hours is involved in 53% of insider IT sabotage cases analyzed with relevant information. Examining case data might help to find a cost-effective solution for this type of insider IT sabotage. However, the generality of solutions from past cases might differ for current or future insider IT sabotage trends.

Intent. This pattern helps organizations to determine if and when to allow remote work based on their mission, need for after-hours work, need for access to services and information after-hours, and their tolerance to process disruptions. Ultimately, this pattern helps organizations to reduce their insider IT sabotage risks.

Example. An employee, upset at the lack of year-end bonuses during a lackluster year for his employer, drinks with co-workers on Thursday night and vents about the lack of the employer's appreciation of his hard work. After arriving home at 2AM, he logs into the employer's system and deletes data critical to the organization's mission. Inadequate backup of the data inhibits the organization's ability to restore the data, resulting in missed deadlines, lost customers, and increased performance problems.

Context. The context for this pattern is that insiders are permitted remote access to organization data, permitted to work outside their NWO, and permitted to work remotely outside NWO.

Problem: **How to benefit from remote NWO workers and minimize risks.** How can organizations benefit from remote employee work without significant risk that remote access will be used counter to the organization's interests? The solution is affected by several forces:

- *Risk of insider IT sabotage:* The primary force driving the solution is the potential for employees to intentionally disrupt an organization's systems and services, or compromise its data.
- *Employee productivity:* Organizations allow employees to work remotely to gain the benefit associated with the extra productivity that accrues.
- *Employee satisfaction:* Flexible remote work options can make it easier for employees to do their job and can increase the organization's ability to attract and retain the best people.

Solution: **Extra monitoring and access control for some NWO remote workers.** Organizations do not need to deny remote access to bring the risk of remote insider IT sabotage to an acceptable level. For instance, remote access can be limited only at particular times of the day, days of the week, and/or times before or after normal working hours. The organization needs to analyze its risks and priorities to make a return-on-investment decision before applying a solution.

The solution for this pattern has the following structure:

(1) Decide which data insiders can legitimately access data via remote IT systems.
(2) Decide the hours within which insiders can legitimately connect to organization systems (e.g., only during normal working hours, only before a preset time, only after a preset time, or plus or minus a number of hours outside of normal working hours). Insiders who travel internationally for work or who work remotely with international teams might legitimately work a wide range of hours, or might legitimately work at all hours.
(3) Decide which days insiders can legitimately connect to organizational systems (e.g., only during their official work days).
(4) Restrict insiders' remote access based on the decisions above.
(5) Explicitly authorize and track remote access paths to organizational systems.
(6) Perform extra monitoring of insider use of remote access paths during elevated risk periods if remote access is allowed. Such monitoring is typically legal. (Always check with legal counsel before setting up targeted increased monitoring, to ensure the monitoring is legal.)

Consequences. We expect the consequence of constrained remote access to be increased prevention of remote insider IT sabotage during high-risk periods.

This pattern has several benefits:

- Employees are allowed to work remotely when they are expected to be most productive.
- Employees are prohibited from working remotely when they are apt to be the most reckless.
- Employees with similar job functions are treated similarly.
- Special provisions for remote work can be made when warranted.

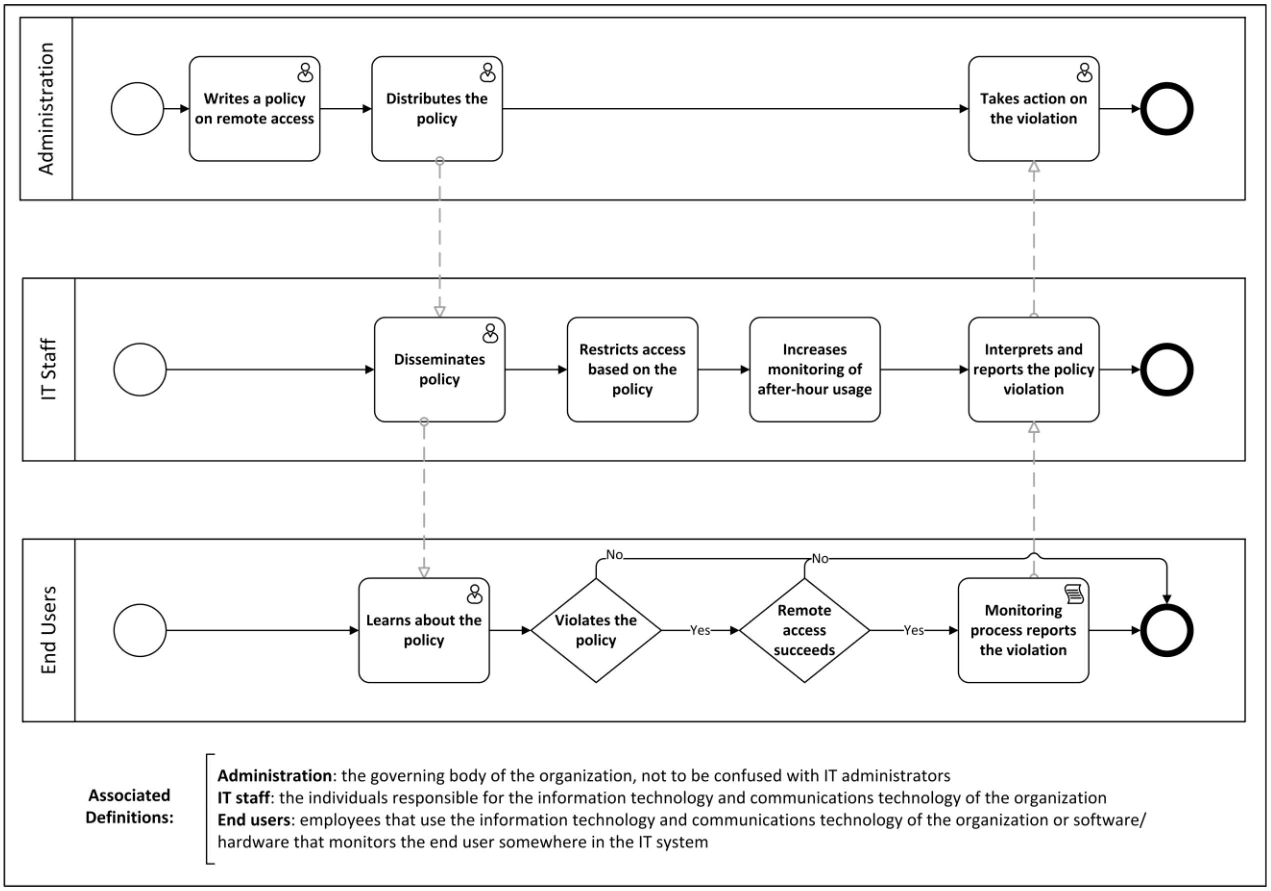
This pattern also has several liabilities:

- Legitimate employee work may be restricted, which may affect productivity.
- Restricting the employee's flexible work options (i.e., ability to work remotely) may reduce employee satisfaction or feelings of mutual trust.
- Employees can wait to attack when remote access is allowed, if the desire to inflict harm persists.

Example Resolved. An employee frustrated over a lack of bonuses tries to log into the organization's system after his late night of drinking, but is denied access because the organization instituted controls to deny access between 10PM and 5AM unless special provisions are authorized by an immediate supervisor.

Other Relevant Patterns. Examining the *Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely* pattern finds that organizations may restrict which users are authorized to log into machines remotely, since IT saboteurs sometimes try to conceal their actions by logging in as others. The *Increase Monitoring for Intellectual Property (IP) Theft by Departing Insiders* [4] pattern was examined for similar attack indicators over a period of a time prior to termination. That pattern, however, examined attack indicators in cases of IP theft rather than insider IT sabotage [9].

Diagram.


Administration
Writes a policy on remote access
Distributes the policy
Takes action on the violation
IT Staff
Disseminates policy
Restricts access based on the policy
Increases monitoring of after-hour usage
Interprets and reports the policy violation
End Users
Learns about the policy
Violates the policy
No
Yes
Remote access succeeds
No
Yes
Monitoring process reports the violation

Associated Definitions:

Administration: the governing body of the organization, not to be confused with IT administrators
IT staff: the individuals responsible for the information technology and communications technology of the organization
End users: employees that use the information technology and communications technology of the organization or software/ hardware that monitors the end user somewhere in the IT system

Figure 1: Sequence Diagram for Pattern 1: Constrain and Monitor Remote Work Outside of Normal Hours

2.2 Pattern 2: *Increase Monitoring Within a Time Window of a Negative Workplace Event.*

Our case data indicate that many insiders who commit insider IT sabotage do so at times close to their date of termination or resignation. This pattern's hypothesis is that insider IT sabotage due to disgruntlement sometimes closely correlates to the time of the negative workplace event that motivates the disgruntlement. For this pattern, we define *resignation* as the date when an insider gives notice of his or her impending termination. *Termination* is the date of the end of the insider's employment with the organization. Resignation is always before or on the same day as the termination day. This pattern involves a negative workplace event within a time window of the insider IT sabotage attack. The length of the time window is something we examine during analysis of case data. Analysis of case data for this pattern is limited to two negative workplace events: termination and resignation.

Design Rationale. Attack incidents are started within 60 days before or after termination or giving resignation notice in 57% of the insider IT sabotage cases analyzed with relevant data. Case data examination might help find a cost-effective solution for this type of insider IT sabotage. Cases with relevant data have termination, resignation, and attack dates. However, the generality of solutions from past cases might differ for current or future insider IT sabotage trends. The temporal relationship of additional negative workplace events and insider IT sabotage attack start times merits further study.

Intent. This pattern helps organizations detect signs of insider IT sabotage and effectively use their IT security resources by increasing monitoring efforts during times when attacks are more likely to occur.

Example. A software engineer is told on Monday that she is being laid off starting next week. She feels that her impending termination is unfair, believing she is a better software engineer than other employees who were not laid off. In anger, she deletes code she wrote and permanently destroys the backup records.

Context. The context for this pattern is that insiders are faced with negative workplace events that may trigger an incident of insider IT sabotage.

Problem: How to cost-effectively mitigate insider IT sabotage risk due to disgruntlement. The solution for this pattern is affected by several forces. Extra monitoring is more expensive (e.g., examining more alerts and extra purchases; installing network sensors or software; approving and implementing extra monitoring by management, IT, etc.). As discussed in the *Introduction*, the risk of insider IT sabotage can be reduced by reducing any of these three factors: *Consequence*, *Vulnerability*, or *Threat*.

In this case, the threat of insider IT sabotage is increased because of the statistical correlation with negative workplace events (i.e., disgruntlement). There are many types of negative workplace events. Some events are due to poor performance by the insider, which might spur the insider's disgruntlement and desire for retribution. Some events may be triggered by external forces, such as a need for layoffs due to a downturn in the economy. Whatever the reason, these forces should be considered when deciding how to deal with negative events and their aftermath.

Solution: Targeted extra monitoring of employees within a time window of a negative workplace event. Organizations may not need to extensively monitor employees within a time window of every negative workplace event to reduce the risk of negative workplace-related insider IT sabotage. An organization should make a return-on-investment-based decision that considers the risks, priorities, and legal limits of the organization before implementing the solution relevant to this pattern. The solution for the *Increase Monitoring Within a Time Window of a Negative Workplace Event* pattern has the following structure:

(1) Determine what the monitoring close to a negative event should examine and how. The content monitored and monitoring techniques used may vary depending on the negative events and laws. (Laws can vary per nation, state, and city; laws and their interpretations may also change over time.)
(2) Scope which "negative workplace events" to include for monitoring. For our pattern, we considered only termination and resignation notice events.
(3) Increase monitoring in the time window prior to termination and resignation.

Consequences. We expect the consequence of increased monitoring is increased and faster detection of insider IT sabotage related to negative workplace events. Another positive consequence could be greater prevention of insider IT sabotage, since a higher likelihood of being caught might act as a deterrent if employees are warned of this type of increased monitoring.

This pattern has an intended benefit:

- Insider IT sabotage due to disgruntlement from a negative workplace event can be detected and responded to early—possibly early enough to prevent costly damage.

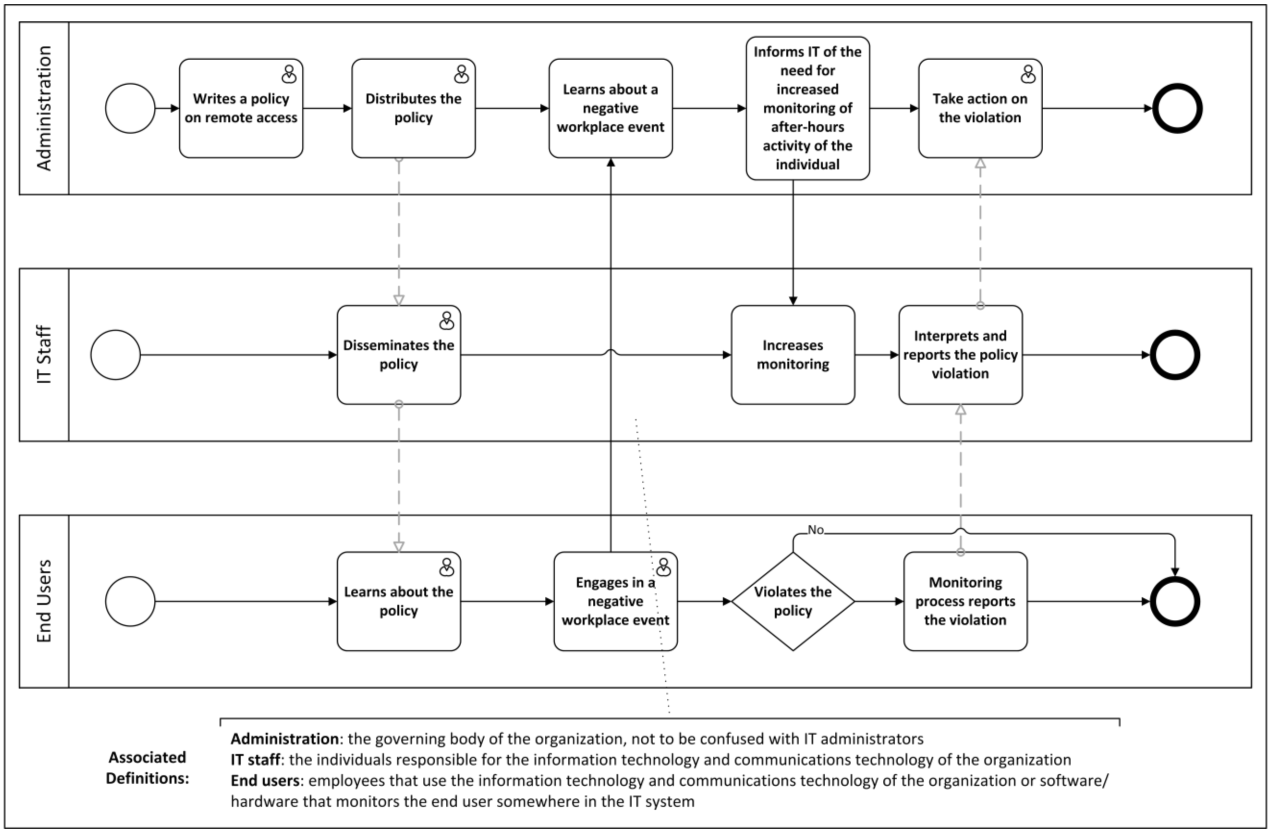
This pattern also has liabilities:

- Innocent and loyal employees may feel untrusted and disrespected due to increased monitoring.
- Increased monitoring has a cost, whether software, hardware, and/or increased worker time.

Example Resolved. An employee, disgruntled over what she feels is an unfair termination scheduled for the end of the week, deletes code she was working on. The monitoring system schedules extra monitoring for unusual behavior by employees with pending terminations. An alert is sent to her manager and the system administrator when the software engineer deletes a large quantity of code. The system administrator quickly freezes the engineer's accounts, and the manager walks her to a secure place and begins a secure early termination process. Backup data still contains the deleted code, which is restored.

Other Relevant Patterns. Examining the *Constrain and Monitor Remote Work Outside of Normal Hours* pattern, organizations may wish to limit remote work outside the worker's normal hours, which might help prevent insider IT sabotage influenced by negative workplace events. Efficiencies can be gained from shared monitoring during overlap periods of recommended monitoring between the two patterns.

Diagram.


Administration
Writes a policy on remote access
Distributes the policy
Learns about a negative workplace event
Informs IT of the need for increased monitoring of after-hours activity of the individual
Take action on the violation
IT Staff
Disseminates the policy
Increases monitoring
Interprets and reports the policy violation
End Users
Learns about the policy
Engages in a negative workplace event
Violates the policy
No
Monitoring process reports the violation

Associated Definitions:

Administration: the governing body of the organization, not to be confused with IT administrators
IT staff: the individuals responsible for the information technology and communications technology of the organization
End users: employees that use the information technology and communications technology of the organization or software/hardware that monitors the end user somewhere in the IT system

Figure 2: Sequence Diagram for Pattern 2: Increase Monitoring Within a Time Window of a Negative Workplace Event

2.3 Pattern 3: *Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely*.

Our case data indicate that some insiders commit IT sabotage via remote access using a co-worker's account. In this pattern, an insider remotely logs in as a co-worker using a machine not affiliated with the co-worker's account.

Design Rationale. In insider IT sabotage cases that have documents that specified which IT account was used, a co-worker's account is involved in 15% of the cases. Fewer used remote access too (details in Section 3). Mitigation for this common attack trend appears inexpensive and simple. However, the generality of solutions from past cases might differ for current or future insider IT sabotage trends.

Intent. This pattern helps organizations determine if attempts to login remotely should not be allowed, to reduce their risk of insider IT sabotage.

Example. An employee who felt offended by a remark a colleague made decides to get even. He uses his work-provided laptop to log in to the work network, but uses *the colleague's* user ID and password. To make his colleague look bad, he inserts errors in documents that will be noticed by valuable customers of the organization.

Context. The context for this pattern is that insiders are permitted remote access to IT systems and the insider has a co-worker's account credentials.

Problem: How to stop employees from remotely using co-worker accounts while benefitting from employee remote work. How can organizations gain the benefit of remote employee work without the remote access being used by malicious individuals to log in under an incorrect user ID, possibly harming a co-worker's reputation as well as the organization's interests? The solution to this pattern is affected by several forces. Employee productivity is higher by allowing them to work remotely, including access to IT systems. Employee satisfaction is linked to flexible work options [13].

Solution: Improved monitoring against remote co-worker account use. The pattern solution includes two parts that should be implemented for both login accounts and VPN accounts:

(1) Track and correlate MAC addresses used for particular user ID logins.
(2) Allow remote login only from MAC addresses correlated to user IDs (i.e., no unknown MAC addresses).

The monitoring, checking, and blocking solution of part (2) is technical and fully automated. A custom solution can be developed if this functionality is not standard in the organization's network systems. The access control solution of part (1) should be done as part of the organization's overall asset identification and access control.

Consequences. We expect the consequence of improved monitoring to be the immediate detection of insider IT sabotage attempts related to remote login attempts using co-worker IDs.

This pattern has several benefits:

- The mitigation is relatively inexpensive.
- Access controls and asset identification for this mitigation are helpful for more cybersecurity uses.
- Mitigation and monitoring should not affect the system user experience unless the user attempts a login against policy.

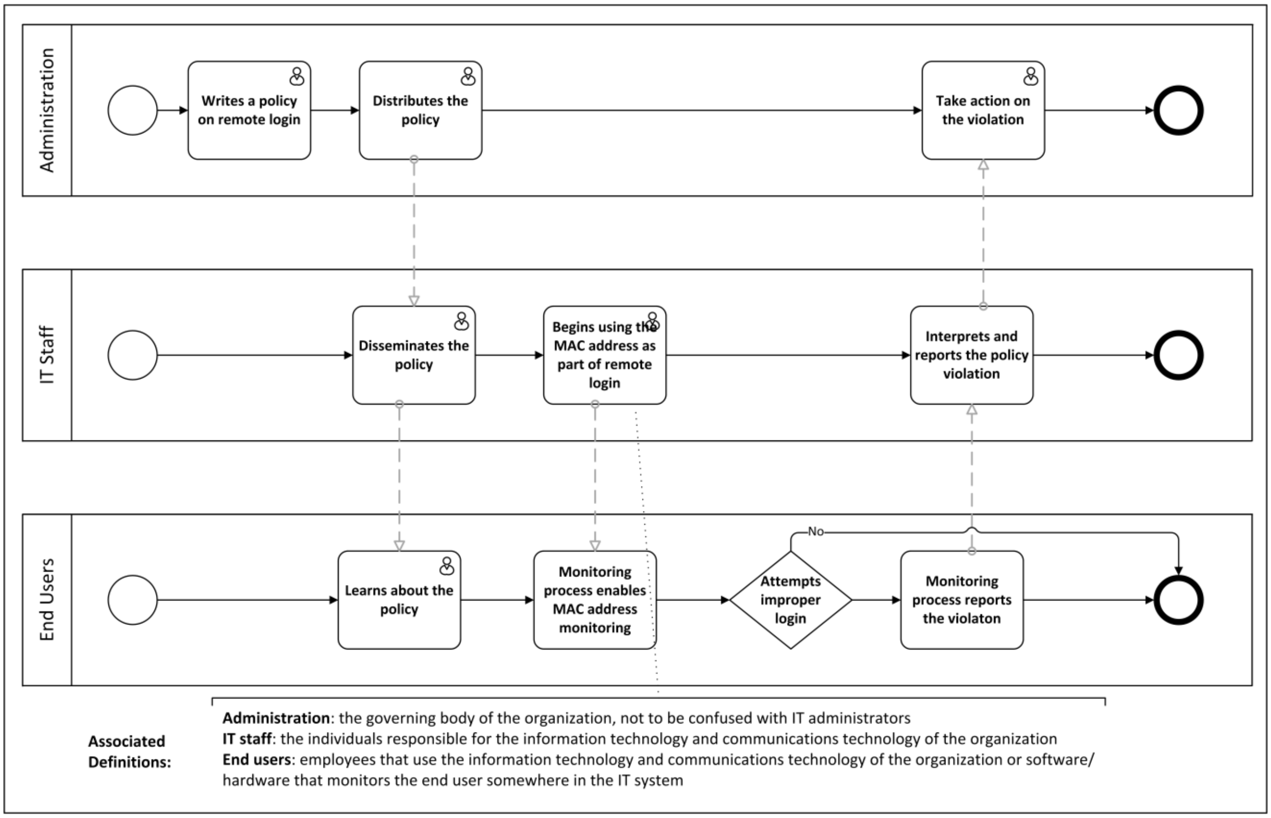
This pattern also has liabilities:

- MAC address spoofing is possible and, although relatively inexpensive, costs something to implement.
- There is a cost required to implement tracking and correlating MAC addresses and user IDs.

Example Resolved. An employee who felt offended tries to log in using a co-worker's user ID. Intrusion detection system (IDS) monitoring equipment prevents his login. The attempt is verified and reported to system administrators and the employee's manager. The manager takes disciplinary action, possibly including termination.

Other Relevant Patterns. The *Increased Monitoring for Intellectual Property Theft by Departing Insiders* [4] pattern uses monitoring of remote access by insiders, but mitigates the problem of IP theft, not insider IT sabotage. Different from *Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely*, it does not guard against and prevent logins. Instead it monitors activity related to successful logins.

Diagram.


Administration
Writes a policy on remote login
Distributes the policy
Take action on the violation
IT Staff
Disseminates the policy
Begins using the MAC address as part of remote login
Interprets and reports the policy violation
End Users
Learns about the policy
Monitoring process enables MAC address monitoring
Attempts improper login
No
Monitoring process reports the violaton

Associated Definitions:

Administration: the governing body of the organization, not to be confused with IT administrators
IT staff: the individuals responsible for the information technology and communications technology of the organization
End users: employees that use the information technology and communications technology of the organization or software/ hardware that monitors the end user somewhere in the IT system

Figure 3: Sequence Diagram for Pattern 3: Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely

2.4 Pattern 4: *Eliminate Potential Methods of Access After Termination.*

Our case data indicate that many insiders who commit IT sabotage do so because of prior disgruntlement or because of job termination. This pattern involves the common problem of an insider attacking an organization's system after the insider's termination. This kind of attack should not be possible if standard termination procedures are followed, since all of the insider's system access should be closed off.

Design Rationale. Access after termination was involved in 63% of insider IT sabotage cases analyzed. Only cases with relevant information were analyzed. (The definition of 'relevant information' is that the case data included information about whether the attack access date was before or after the date of termination, information about the attack date, and information about the termination date. The information about the attack and termination date did not need to be precise to the day; however, it did have to be precise enough to confirm that the attack was post-termination. Examining cases might provide data for finding cost-effective solutions for this type of insider IT sabotage. However, solutions derived from analysis of past cases might not be useful for current or future cases.

Intent. This pattern helps organizations avoid insider IT sabotage after the insider leaves the organization.

Example. The organization's chief technical officer (CTO) was fired for poor performance. The next week she logged into a system administrator account and inserted a logic bomb into the backup system designed to delete all of the organization's backups.

Context. The context for this pattern is that insiders access their organization's IT systems after their termination and departure from the organization.

Problem: How to stop employee access to organization's IT systems after termination. Our case data indicate that many insiders who commit insider IT sabotage do so because of disgruntlement leading to termination or because of job termination. The solution to this pattern is affected by several forces. The termination procedure must be implemented. Minimizing risk can involve limiting the organization's vulnerability to the post-termination type of insider IT sabotage.

Solution: Eliminate potential methods of access after termination. To eliminate potential methods of access after termination, the pattern solution has four parts:

(1) Ensure that a comprehensive termination procedure is used throughout the organization. The termination procedure should have the following characteristics:
   a. be well known throughout organization
   b. include retrieving all hardware and remote access tokens
   c. require closing all of the insider's accounts and current connections
   d. include password changes on all remaining password accounts, including shared accounts, network devices, and test accounts
   e. comprehensively remove access, including keys and badges
   f. ensure that news of the termination is communicated to all co-workers

(2) Establish a process that tracks all accounts assigned to each employee.
(3) Explicitly authorize and track remote access paths, which are defined as a sequence of one or more access points that lead to a critical system [11].
(4) Monitor remote and local access by insiders.

Consequences. We expect the consequence of implementing a comprehensive termination procedure in combination with account tracking and access control and monitoring to be prevention and detection of insider IT sabotage attempts post-termination.

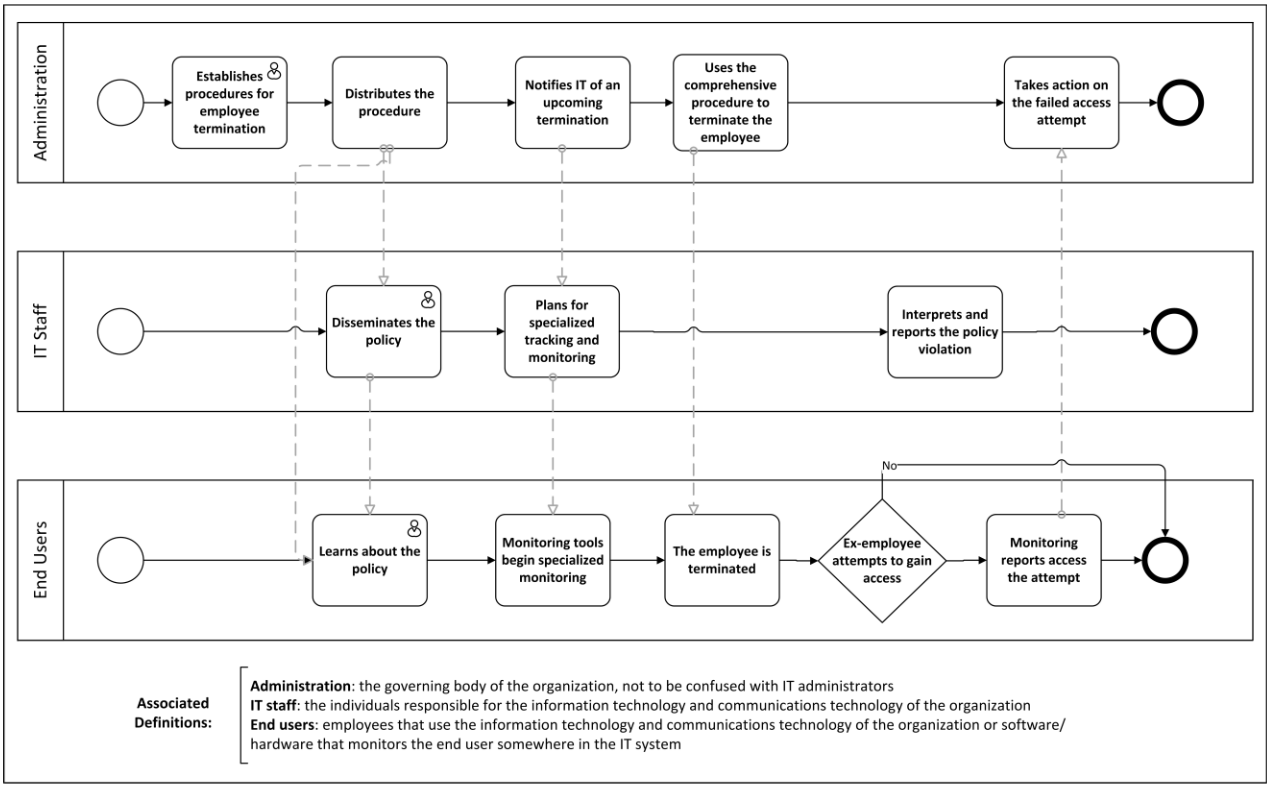
This pattern has a liability:

- There is a cost to comprehensively removing an employee's access during and immediately after termination.

Example Resolved. The ex-CTO attempted to access to her system administrator account, but was unable to log in because the organization thoroughly removed her access to her accounts as part of the comprehensive termination procedure. An alert was sent to the current system administrator and management, who alerted law enforcement officials to the issue of the attempted unlawful login.

Other Relevant Patterns. The *Increased Monitoring for Intellectual Property Theft by Departing Insiders* [4] pattern has a common attack indicator (via remote access). However, the new pattern has many differences because it includes system access via remote access for a period of a time prior to termination, specifies access outside normal work hours, and prevents insider IT sabotage instead of IP Theft.

Diagram.


Administration
Establishes procedures for employee termination
Distributes the procedure
Notifies IT of an upcoming termination
Uses the comprehensive procedure to terminate the employee
Takes action on the failed access attempt
IT Staff
Disseminates the policy
Plans for specialized tracking and monitoring
Interprets and reports the policy violation
End Users
Learns about the policy
Monitoring tools begin specialized monitoring
The employee is terminated
Ex-employee attempts to gain access
No
Monitoring reports access the attempt

Associated Definitions:

Administration: the governing body of the organization, not to be confused with IT administrators
IT staff: the individuals responsible for the information technology and communications technology of the organization
End users: employees that use the information technology and communications technology of the organization or software/hardware that monitors the end user somewhere in the IT system

Figure 4: Sequence Diagram for Pattern 4: Eliminate Potential Methods of Access After Termination

3. INITIAL EFFECTIVENESS ANALYSIS

3.1 Methodology for Initial Pattern Effectiveness Analysis

From the CERT Division's insider threat database, 46 insider IT sabotage cases were analyzed. Source documents identified during the coding process were used, but data entry relied directly on information in source documents. Source documents included court documents, news stories, and investigator notes. Four coders entered data into a formatted spreadsheet using guidelines provided by a coding guidebook. Supporting data was found in the initial analysis of case data. Some of the coding fields could not be completed using the data sources for some cases because relevant information was missing.

Table 1: Pattern Terminology Definitions and Notations

Variable Description	Notation	Definition
Remote Access	RA	Refers to an insider who performs work tasks outside the physical boundaries of the organization's buildings (e.g., VPN while working from home)
Outside Normal Working Hours	ONW	Refers to an insider who connects to an IT system outside of her/his individual normal working days/hours (e.g., if normal working hours for an insider is M-F, 11AM-7PM and the insider connects at 8AM)
Time of Day	ToD	Refers to cases with information about the time of day when the incident took place (e.g., 3 PM)
Days of Week	DoW	Refers to cases that include information about the day of the week when the incident took place (e.g., Friday)
Job Categories	JC	Refers to cases that include the insider's job category (e.g., Information Technology)
Incident Cost	IC	Refers to cases that include the cost associated with the incident (e.g., $50,000)
Co-worker's ID	CwID	Refers to an insider who used a co-worker's login ID to log into a system
Co-worker's Password	CwPwd	Refers to insider who used a co-worker's password (with the co-worker's ID) to log into a system
Co-worker's Account	CwA	Refers to an account owned by another employee of the same organization (e.g., colleague)
Co-worker's Assigned Machine	CwMAC	Refers to a machine assigned to another employee of the same organization (e.g., colleague)
Access after Termination	AaT	Refers to an insider who had access to system(s) after termination
Access after Resignation	AaR	Refers to an insider who had access to system(s) after he/she resigned
Date of Termination	DoT	Refers to cases that include the date when the insider was terminated from the organization
Date of Resignation	DoR	Refers to cases that include the date when the insider resigned from the organization
Date of Incident	DoI	Refers to cases that include the date when the incident occurred

3.2 Terminology and Definitions for Initial Pattern Effectiveness Analysis

Terminology is defined in Table **1**: Pattern Terminology Definitions and Notations; these definitions and notations are used in tables 2-6, which summarize data for the patterns.

Each pattern table (tables 2-5) provides the pattern number and a brief description of the pattern. The *description* column is split into two sub-columns: *Info About* and *Matches*. The *Info About* field sub-column contains notations that represent particular data categories that were collected from cases. For example, if a case has information about the Remote Access (RA) data category (even if the information for the RA data category is that the saboteur's access was local, not remote), then the case is considered to have *Info About* RA.

These data were used for analysis of cases with particular types and combinations of information. The *Matches* field contains notations that identify the cases for a pattern that we consider only with a particular value of the data investigated. For example, for RA, only cases that involved attacks via remote access are a match; similarly, for ONW, only attacks that started outside of normal working hours are a match.

The *Number of Cases Meeting Description* column lists the aggregate number of cases that meet the description in the *Info About* and *Matches* sub-columns. The *Total Number of Cases Analyzed* column lists the entire dataset of cases that we looked at or a subset of the dataset, depending on the description. The *Percentage* field shows the number of cases meeting the description divided by total number of analyzed cases. (For example, in Table 2, the top row indicates that 32 of the 46 cases analyzed have information about whether the attack included remote access or not. So 70% of the cases had data about remote access. The *fifth* row of the table matches the attack addressed by mitigation Pattern 1, when the attacker used remote access while outside the individual's normal working hours, but only for cases that also have data about the incident time of day.)

3.3 Data Analysis of Pattern 1: *Constrain and Monitor Remote Work Outside of Normal Hours.*

To confirm our hypothesis that a majority of insiders complete their attacks remotely outside of their normal working hours, and particular times and days of the week benefit from targeted monitoring more than others, we analyzed the data in Table 2. The data show that a majority of insiders completed their attacks remotely. We saw a number of cases that included information about both outside normal working hours and remote access. Therefore, a resulting hypothesis is that extra monitoring for remote access by users working outside their normal hours might be a useful risk reduction strategy.

Table 2: Pattern 1 - Constrain and Monitor Remote Work Outside of Normal Hours

Pattern 1: Constrain and Monitor Remote Work Outside of Normal Hours				
Description		Number of Cases Meeting Description	Total Number of Analyzed Cases	Percentage
Info About	Matches			
RA		32	46	70%
ONW		17	46	37%
RA & ONW		17	46	37%
ToD		7	46	15%
ToD & RA & ONW		7	46	15%
ToD & RA & ONW	RA & ONW	4	46	9%
DoW		29	46	63%
DoW & RA & ONW		15	46	33%
DoW & RA & ONW	RA & ONW	8	46	17%
JC		39	46	85%
JC & RA & ONW		14	46	30%
JC & RA & ONW	RA & ONW	7	46	15%
IC		33	46	72%
IC & RA & ONW		16	46	34%
IC & RA & ONW	RA & ONW	8	46	17%
IC & RA & ONW	RA & ONW	8	16 (info about IC & RA & ONW)	50%
RA & ONW	RA & ONW	9	17 (info about RA & ONW)	53%
DoW & RA & ONW	RA & ONW	8	15 (info about DoW & RA & ONW)	53%
JC & RA & ONW	RA & ONW	7	14 (info about (re.) JC & RA & ONW)	50%

Figure 5 shows the attack start per days of the week. Weekends show far fewer attack starts, with none on Saturdays. Wednesday had the most and Tuesday the least weekday attack starts. These data are consistent with the pattern hypothesis that particular days of the week benefit from targeted monitoring more than others. Given the large percentage of unknown-day attack starts, true relative risks per day of the week for attack starts might vary significantly from what is shown. Thus, the pattern hypothesis for days of the week is weakly supported, but more data is needed to make firm conclusions.

Figure 6 shows the frequencies of incident (attack) start times. Attack times around midnight occur four times more frequently than attacks in the other time ranges. These data are consistent with the pattern hypothesis that extra monitoring at those times for attack starts could be a cost-effective mitigation strategy. However, a relatively low number of our cases have known attack start times, and more information is needed to make firm conclusions.

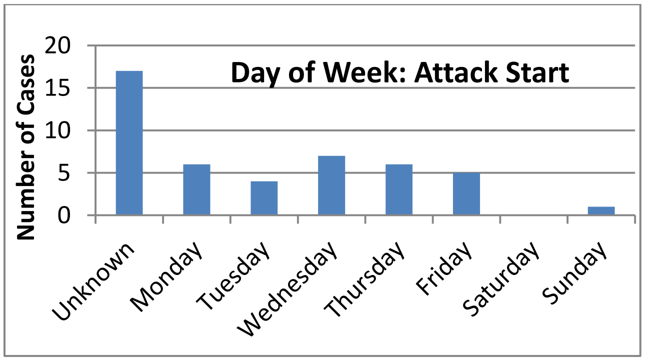


Figure 5: Attack Start Days of Week, Including Unknown

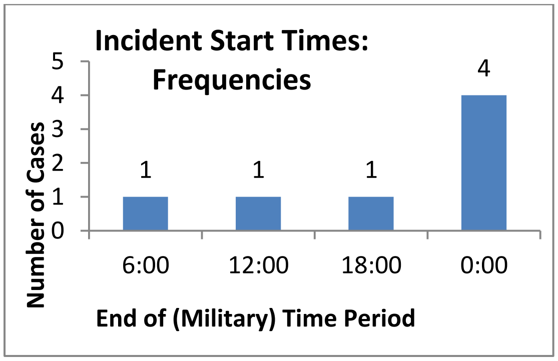


Figure 6: Frequencies of Incident Start Times

3.4 Data Analysis of Pattern 2: *Increase Monitoring Within a Time Window of a Negative Workplace Event.*

To confirm our hypothesis that to increase monitoring within a time window of a negative workplace event will help organizations to prevent, detect, and respond to insider IT sabotage threats, we analyzed the data in Table 3. These data are associated with the fourth pattern we developed, namely, termination or resignation. Termination and resignation have a significant correlations with the dates of initial insider IT sabotage attempts. The data show a majority of cases had information regarding termination and/or resignation dates. We found that 85% of cases had incident date information. A resulting hypothesis is that data measuring differences between termination and incident dates could help organizations narrow the monitoring timeframe.

Table 3: Pattern 2 - Increase Monitoring Within a Time Window of a Negative Workplace Event

Pattern 2: Increase Monitoring Within a Time Window of a Negative Workplace Event				
Description		**Number of Cases Meeting Description**	**Total Number of Analyzed Cases**	**Percentage**
Information About	Matches			
DoT		29	46	63%
DoR		3	46	7%
DoT and/or DoR (no double-counted cases)		29	46	63%
DoI		39	46	85%
DoI & DoT		27	46	59%

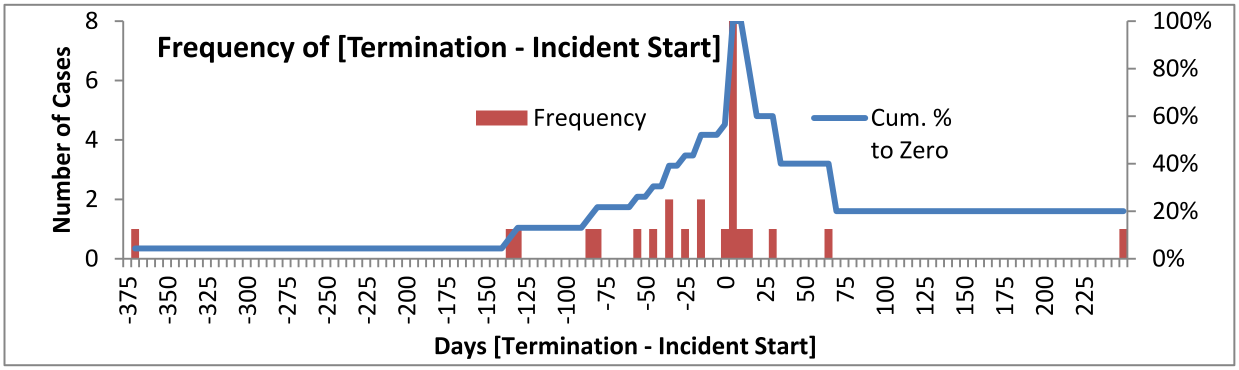


Figure 7: Frequency of [Termination Date - Incident Start Date] in Number of Days, in Number of Cases, and in Cumulative Percent

Figure 7 shows the frequency of [termination – attack incident start], in number of days between the two dates. The red bars show the cumulative number of cases for each number of days from termination to attack. Where data were known, the majority of attacks happened on the day of termination. In most other cases, attacks occurred close to the termination date and most attacks started after termination. The blue line shows the cumulative percentages of total attacks as calculated separately on positive and negative sides of the x axis, summing from either side to 100% at x=0. The cumulative percentage calculations both before and after the attack include attacks that occurred the same day as termination. There were 15 cases that started after termination, 5 cases that started before termination, and 8 cases that started on the day of termination.

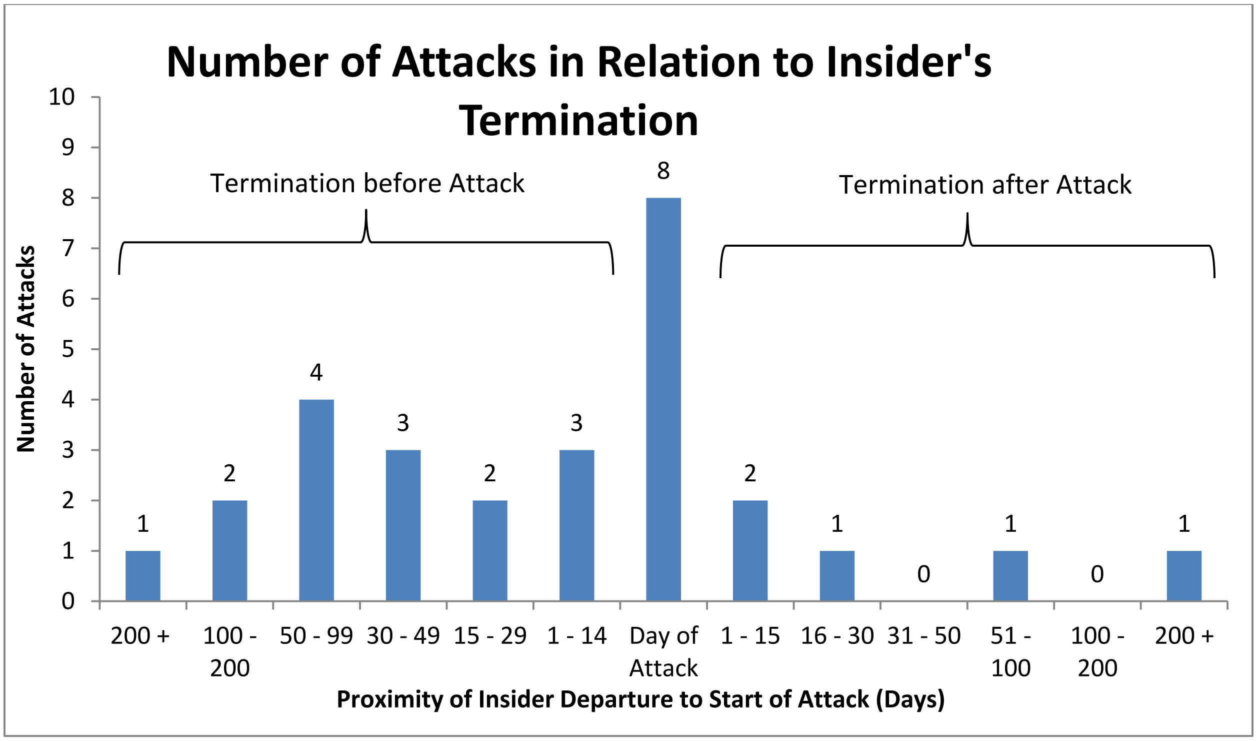


Figure 8: Number of Attacks in Relation to Days from Insider's Termination (Missing cases had insufficient data)

Figure 8 shows another view of the values for known [termination – attack incident start] dates, in number of days between the two dates on the y axis. This view enumerates the 46 cases that were studied on the x axis. The majority of cases with data show attacks starting very close to the termination date, and mostly after termination, although a couple of outliers exist. The two outliers are cases 15 and 23; otherwise, all cases occurred within 141 days of termination.

These data support prevention and detection methods that include increased monitoring of insider activities close to the date of the insider's termination. Detecting attacks earlier can help organizations reduce or prevent damage from attacks. Case data support the pattern's mitigation, which requires consistent, secure termination procedures. These procedures eliminate the terminated insider's access to the organization's data and systems, thus eliminating the employees' ability to commit post-termination IT sabotage.

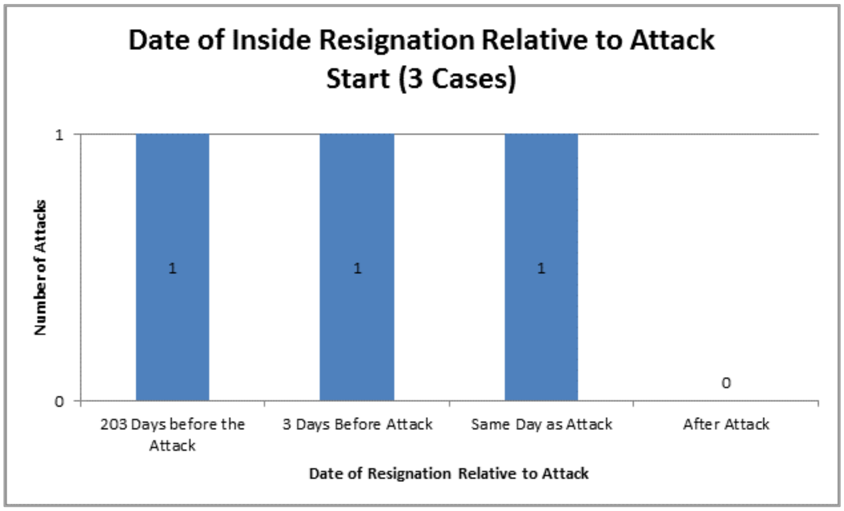


Figure 9: Date of Insider Resignation, Relative to Attack Start (Days)

Figure 9 shows the values for known dates of insider resignation, relative to the attack start date, versus the 46 cases on the x axis. Attack starts were 0, 3, and 203 days after resignation for the 3 known resignation dates. These data support prevention and detection methods that include increased monitoring of insider activities close to the date of the insider's resignation, although not as strongly as the termination data indicate. There are less data, and 1 of the 3 data points available shows a long time between dates. The data support the pattern's mitigation, which requires secure termination procedures. Three data points are obviously insufficient to draw a conclusion.

3.5 Data Analysis of Pattern 3: Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely.

To confirm our hypothesis that organizations are not protecting against insiders who remotely log in with a co-worker's ID and password using standard security practices such as MAC address matching, we analyzed the data in Table 4.

Table 4: Pattern 3 - Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely

Pattern 3: Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely				
Description		Number of Cases Meeting Description	Total Number of Analyzed Cases	Percentage
Info About	Matches			
RA		32	46	70%
RA & [(CwID & CwPwd) from CwMAC]		4	46	9%
RA & [(CwID & CwPwd) from CwMAC]	[(CwID & CwPwd) from CwMAC]	2	46	4%
CwA		6	46	13%
RA & (CwID & CwPwd) from ~ CwA	RA & (CwID & CwPwd) from ~ CwA	2	4 (info re. RA & [(CwID & CwPwd) from CwMAC]	50%

Table 4 shows Pattern 4 cases whereby an organization was either unaware of this capability and/or decided against implementing it. Since there are at least 2 of 46 cases [4%] that include remote access with a co-worker ID and password from a MAC address mismatch, we hypothesize that we can reduce this threat by forcing MAC address matching for remote access users. Also, better security awareness training and controls could prevent insiders from learning co-workers' passwords.

The data points examined are (1) if the login used for the attack was from a remote place and (2) whether a co-worker's ID and password were used to log in. There were 32 cases with information about if a remote login was part of the attack. However, only 4 of the cases involved a remote login using a co-worker's user ID and password. Of those, 2 cases used a machine that was not assigned by the organization to the co-worker.

3.6 Data Analysis of Pattern 4: Eliminate Potential Methods of Access After Termination.

To confirm our hypothesis that a more effective, consistent implementation of comprehensive secure termination procedures would help organizations to prevent, detect, and respond to insider IT sabotage threats, we analyzed the data in Table 5. The data show that more than half the cases involve insiders gaining access after termination. Furthermore, many cases (85%) had information pertaining to the insider's job description. Therefore, a resulting hypothesis is that organizations may benefit from more effective, consistent implementation of comprehensive secure termination procedures for terminations, particularly targeting employees that fit into specific job categories.

Table 5: Pattern 4 - Eliminate Potential Methods of Access After Termination

Pattern 4: Eliminate Potential Methods of Access After Termination				
Description		**Number of Cases Meeting Description**	**Total Number of Analyzed Cases**	**Percentage**
Information About	**Matches**			
AaT		27	46	59%
AaT	AaT	17	27 (info re. AaT)	63%
IC		33	46	72%
AaT & IC	AaT	14	33 (info re. IC)	42%
JC		39	46	85%
JC & AaT		24	46	52%
JC & AaT	AaT	14	46	30%
ToD		7	46	15%
ToD & AaT	AaT	5	46	11%
ToD & AaT	AaT	5	7 (info re. ToD)	71%
DoW		29	46	52%
DoW & AaT	AaT	15	46	33%

4. COSTS

Table 6 shows the average incident cost for each pattern and for all cases, which were derived from associated costs identified in the case data. The average for all cases is higher because it includes high-incident-cost cases that do not match the four patterns. The resulting hypothesis is that using cost data for risk-related decisions allows organizations to make better use of resources for mitigating insider threats.

Table 6: Average Incident Cost Information for Each Pattern, and for All Cases

Pattern?	**Avg. Cost**
All Insider IT Sabotage Cases (Pattern Matches and Not)	$278,000
1: Constrain Remote Work Outside of Normal Hours	$182,000
2: Increase Monitoring Within a Time Window of a Negative Workplace Event	$18,500
3: Monitor for Insiders' Machines Using Co-Workers' Accounts Remotely	$191,000
4: Eliminate Potential Methods of Access After Termination	$216,000

5. INFORMATION NEEDED

5.1 INTER-RATER RELIABILITY (IRR)

Inter-rater reliability measures the degree of agreement between multiple coders who evaluate the same data and reach a conclusion. A *coder* is a person who uses source information (e.g., documents, interviews, recordings) and enters select data from the source information into fields specified for a project. The similarity between the conclusions reached by the coders is a positive indicator in the inter-rater reliability process. This reliability is essential to validate subjectively coded data in research analysis.

An example of dissimilar conclusions is when two coders read the same investigator notes document from an insider IT sabotage case and one coder concludes that the attack happened *during* normal working hours but the other coder concludes the attack happened *outside* normal working hours.

For our project, the coder uses source documents that may be investigator notes, court documents, or news articles to enter information into a spreadsheet with specified fields. The information the coder enters is specified in the source document, but is entered into the spreadsheet using definitions and coding guidance provided in a coding guide. Many of the fields have a limited number of drop-down menu options for the coder, but other fields allow the coder to fill in text freely.

Once coders evaluate the information, it must be systematized numerically and then the inter-rater reliability can be calculated using well-known statistical analyses such as Cohen's kappa, Fleiss' kappa, and nominal Krippendorff's alpha [17]. A higher score generally means that the coders had more similarities in conclusions, and if the value is high enough, it indicates an acceptable IRR.

Accepted threshold values vary per researcher and type of statistical analysis, but "coefficients of .90 or greater are nearly always acceptable [and] .80 or greater is acceptable in most situations" [18]. This process ensures the accuracy of coded information that can be used to conduct analyses. A low or missing IRR score does not account for possible discrepancies in coding information, and is not as reliable as information that has undergone an IRR with positive results [17]. The case coding used in this preliminary analysis has not passed an IRR test with an acceptable value.

5.2 BASELINE DATA

Baseline data are defined in this research as a measurement of the same data for individuals who did not (as far as we know) commit IT sabotage that are used as a basis for comparison with those who did. Baseline data are an important factor to take into consideration prior to reaching conclusions. Without comparison to a baseline, data may seem relevant to analysis and conclusions, but in reality might not be.

For example, a previous analysis of the CERT Division's insider threat database determined that for database cases, 30% of insiders who committed IT sabotage had a previous arrest history. This information might sound significant without examining the baseline data, which show that 30% of all U.S. adults have been arrested by age 23, based on a 2011 study using information from the U.S. federal government [8]. Thus, after incorporating the baseline data, the (otherwise same) data analysis does not find any connection between previous arrest and the tendency to commit IT sabotage. Thus, the data do not support background checks of arrest records prior to hiring or promotion. Baseline data is important to understand prior to making data-driven conclusions. Baseline data has not yet been gathered to compare to the IT sabotage data coded in this project.

6. DISCUSSION

Four insider IT sabotage patterns were described and an initial effectiveness analysis was provided based on the analysis of 46 real-world adjudicated insider IT sabotage cases. Supporting data were found in the initial analysis of case data. More case coding is required for more rigorous analysis, as conclusive results cannot be drawn due to insufficient data for analysis, a lack of baseline data, and lack of a sufficient IRR score.

Baseline data for assumed non-malicious insider populations should be a subject of future study, as well as work to achieve strong IRR scores for coding. Large quantities of insider IT sabotage case data might be hard to obtain, but collaboration with corporations and law enforcement organizations might help. In the future, more consideration should be given to the return on investment for each pattern in case data analysis; perhaps organizations would benefit from looking at risky events specific to them to select which patterns to use, otherwise some mitigation patterns could cost more than what is lost due to IT sabotage. Organization size might correlate with the effectiveness of one or more of the mitigation patterns. Also, mitigation pattern effectiveness may vary given conditions within particular countries, due to factors of relevant local laws, culture, technology, corruption, and law enforcement [19].

7. ACKNOWLEDGEMENTS

The authors thank David Zubrow, Robert Stoddard, and Will Hayes of the SEI for their quantitative analysis insights, and Merly Knox and Alicia Kozakiewicz for many hours of insider threat case coding. We are grateful to Dr. David West, our paper's official PLoP shepherd, who provided excellent comments and recommendations that significantly improved this paper. We thank the members of our PLoP 2013 workshop for their close reading of the paper and helpful suggestions for edits. We also thank our professional editor, Sandy Shrum, for her improvements to this paper.

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. This material has been approved for public release and unlimited distribution.

REFERENCES

[1] J. Espenschied, "A Discussion of Threat Behavior: Attackers & Patterns," Microsoft Corporation, Seattle, WA, 2012.

[2] L. Frank & R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *Journal of Strategic Security,* vol. 4, no. 2, p. 3, 2011.

[3] A. P. Moore, *et al.*, "A Preliminary Model of Insider Theft of Intellectual Property," Software Engineering Institute, Pittsburgh, PA, 2011.

[4] A. P. Moore, M. Hanley, & D. Mundie, "A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders," *Proc. Conf. Pattern Languages of Programs,* 2011, pp. *1–17.*

[5] D. Mundie, A. P. Moore, & D. McIntire, "Building a Multidimensional Pattern Language for Insider Threats," *Proc. Conf. Pattern Languages of Programs,* 2012.

[6] M. Schumacher, *et al., Security Patterns: Integrating Security and Systems Engineering,* vol. 7. Hoboken, NJ: Wiley, 2006.

[7] D. Mundie, *et al.* "Effectiveness of a Pattern for Detecting Intellectual Property Theft by Departing Insiders," Software Engineering Institute, Pittsburgh, PA, 2012.

[8] G. Silowash, *et al.*, "Common Sense Guide to Prevention and Detection of Insider Threats (4th ed.)," Software Engineering Institute, Pittsburgh, PA, 2012.

[9] M. Hanley & J. Montelibano, "Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination," Software Engineering Institute, Pittsburgh, PA, 2011.

[10] C. Kohls & S. Panke, "Is that true …?: Thoughts on the Epistemology of Patterns," *Proc. 2009 Conf. Pattern Languages for Programs*, 2009.

[11] D. Cappelli, A. Moore, & R. Trzeciak, *The CERT Guide to Insider Threats*, Boston, MA: Addison-Wesley Professional, 2012.

[12] L. A. Cox Jr., "Some limitations of Risk= Threat× Vulnerability× Consequence for Risk Analysis of Terrorist Attacks," *Risk Analysis* vol. 28., no. 6. pp. 1749-1761, 2008.

[13] C. Kelliher & D. Anderson. "Doing More with Less? Flexible Working Practices and the Intensification of Work," *Human Relations,* vol. 63, no. 1, pp. 83-106, 2010.

[14] R. Buschmann, K. Henney, & D. Schmidt, *Pattern-Oriented Software Architecture, On Patterns and Pattern Languages*, vol. 5. Hoboken, NJ: Wiley, 2007.

[15] F. Buschmann, K. Henney, & D. C. Schmidt, *Pattern-Oriented Software Architecture Volume 4: A Pattern Language for Distributed Computing*, vol. 4. Hoboken, NJ: Wiley, 2007.

[16] C. Alexander, S. Ishikawa, & M. A. Silverstein, *Pattern Language: Towns, Buildings, Construction*, New York, NY: Oxford University Press, 1977.

[17] D. G. Freelon, "ReCal: Intercoder Reliability Calculation as a Web Service," *Int. Journal of Internet Science,* vol. 5, no. 1, pp. 20–33, 2010.

[18] M. Lombard, J. Snyder-Duch, & C. Campanella Bracken, *Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Research Projects* [Online]. Available: http://ils.indiana.edu/faculty/hrosenba/www/Research/methods/lombard_reliability.pdf. (URL)

[19] L. Flynn, C. Huth, R. Trzeciak, & P. Buttles-Valdez. "Best Practices Against Insider Threats in All Nations", CMU/SEI-2013-TN-023. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2013.