A Preliminary Model of Insider Theft of Intellectual Property

Andrew P. Moore
CERT Program[*]
Software Engineering Institute
4555 Fifth Avenue
Pittsburgh, PA 15213
apm@cert.org

Dawn M. Cappelli
CERT Program
Software Engineering Institute
4555 Fifth Avenue
Pittsburgh, PA 15213
dmc@cert.org

Thomas C. Caron[†]
Deloitte Consulting
Boston, MA
tcaron@gmail.com

Eric Shaw, Ph.D.
Consulting and Clinical Psychology, Ltd.
Suite 514
5225 Connecticut Ave., NW
Washington, DC 20015
eshaw@msn.com

Derrick Spooner
CERT Program
Software Engineering Institute
4555 Fifth Avenue
Pittsburgh, PA 15213
dspooner@cert.org

Randall F. Trzeciak
CERT Program
Software Engineering Institute
4555 Fifth Avenue
Pittsburgh, PA 15213
rft@cert.org

Abstract

A study conducted by the CERT Program at Carnegie Mellon University's Software Engineering Institute analyzed hundreds of insider cyber crimes across U.S. critical infrastructure sectors. Follow-up work involved detailed group modeling and analysis of 48 cases of insider theft of intellectual property. In the context of this paper, insider theft of intellectual property includes incidents in which the insider's primary goal is stealing confidential or proprietary information from the organization. This paper describes general observations about and a preliminary system dynamics model of this class of insider crime based on our empirical data. This work generates empirically-based hypotheses for validation and a basis for identifying mitigating measures in future work.

Key Words: Information Security, Insider Threat, Theft of Intellectual Property, Modeling, System Dynamics, Theft of Information

1 Introduction

Since 2002, the CERT Program at Carnegie Mellon University's Software Engineering Institute has been gathering and analyzing actual malicious insider incidents, including information technology (IT) sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to the critical infrastructure of the United States. Consequences of malicious insider incidents include financial losses, operational impacts, damage to reputation, and harm to individuals. The actions of a single

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 1, pp. 28-49

[*]CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

[†]Tom Caron's contributions to this paper occurred as a student at the H. John Heinz III College, School of Information Systems Management, Carnegie Mellon University.

insider have caused damage to organizations ranging from a few lost staff hours to negative publicity and financial damage so extensive that businesses have been forced to lay off employees and even close operations. Furthermore, insider incidents can have repercussions beyond the affected organization, disrupting operations or services critical to a specific sector, or creating serious risks to public safety and national security.

CERT's insider threat work, referred to as MERIT (Management and Education of the Risk of Insider Threat), uses the wealth of empirical data collected by CERT to provide an overview of the complexity of insider events for organizations—especially the unintended consequences of policies, practices, technology, efforts to manage insider risk, and organizational culture over time. As part of MERIT, we have been using system dynamics modeling and simulation to better understand and communicate the threat to an organization's IT systems posed by malicious current or former employees or contractors. Our work began with a collaborative group modeling workshop on insider threat hosted by CERT and facilitated by members of what evolved into the Security Dynamics Network and the Security Special Interest Group. [1]

Based on our initial modeling work and our analysis of cases, we have found that different classes of insider crimes exhibit different patterns of problematic behavior and mitigating measures [2]. CERT has found four categories of insider threat cases based on the patterns we have seen in cases identified: IT sabotage, fraud, theft of intellectual property (IP), and national security espionage. We believe that modeling these types of crimes separately can be more illuminating than modeling the insider threat problem as a whole. In this paper, we focus on theft of IP.

We define insider theft of IP as crimes in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data to steal confidential or proprietary information from the organization.[1] This paper is centered on two dominant models found within the cases: the Entitled Independent Scenario (27 cases) and the Ambitious Leader Scenario (21 cases). We first define our approach to building these models. Next, we incrementally build the models describing them as we go. Finally, we provide general observations and discuss future work. Appendix A summarizes important characteristics of the crimes involving theft of IP. Appendices B and C provide an overview of the models developed. We believe that these models will help people better understand the complex nature of this class of threat. Through improved understanding comes better awareness and intuition regarding the effectiveness of countermeasures against the crime. Our work generates strong hypotheses based on empirical evidence. Future work will involve alignment with existing theory, testing of these hypotheses based on random sampling from larger populations, and analysis of mitigation approaches.

2 Related Work

There is a vast literature on counterproductive work behavior (CWB), which is defined as "any intentional behavior on the part of an organizational member viewed by the organization as contrary to its legitimate interests" [4]. This includes a wide variety of both self-destructive and retaliatory behaviors, but specifically encompasses, sabotage, stealing, fraud, and vandalism. Sackett and DeVore provide a thorough literature review and group the antecedents into personality variables, job characteristics, work group characteristics organizational culture, control systems, and injustice.[5] This work supports our findings of personal predispositions and organizational and individual stressors as antecedents of a range of malicious activity. Our past work has involved modeling insider fraud [6] and insider IT sabotage [7] [8].

[1] While some frameworks include accidental harmful acts within the scope of insider threat [3], the CERT's past and present work has focused only on intentional acts by an insider.

The primary personality model used in CWB research is the Five Factor Model (FFM). The FFM includes dimensions of openness to experience, extraversion, conscientiousness, agreeableness, and emotional stability. After reviewing the literature on the FFM dimensions and CWBs, Salgado found 44 studies conducted between 1990 and 1999 that examine the relationship between the FFM dimensions and deviant behaviors (17), absenteeism (13), work related accidents (9), or turnover (5).[9] This work showed that conscientiousness and agreeableness were significant, valid predictors of workplace deviance. Related work showed that workplace stress [10] and insider perceived status within the organization [11] were correlated with CWBs.

The personal, situational, and behavioral antecedents identified in the CWB literature are also supported in many models of computer-related malicious insider activity:

- the Capability, Motive, Opportunity Model [12] [13]
- behavioral models [14] [15]
- an entity relationship model in a comprehensive characterization framework [16]
- a criminological and social model [17]

One effort developed a system dynamics model to compare the problem domains of IT sabotage and espionage to identify similarities and differences between the two classes of crimes [18]. This study was based on the espionage and insider threat data collected by the Defense Personnel Security Research Center (PERSEREC) [19] [20] [21]. In addition, social science experiments within organizations, such as those conducted at Mitre [22], can help validate hypotheses about the problem generated through empirical work such as described in this paper, as well as test deterrent measures against the threat patterns seen.

3 Approach

Our research approach is based on the comparative case study methodology [23]. The cases we selected fit the above definition of theft of IP. We identified these cases through public reporting and included primary source materials, such as court records in criminal justice databases (found through searches on Lexis court databases), and other secondary source materials such as media reports (found through searches on Lexis-Nexis news databases and Internet search engines such as Google).

We used the following criteria to select cases:

- The crime occurred in the United States.
- The subject of the crime was prosecuted in a United States court.
- Sufficient quantities and quality of data were available to understand the nature of the case.

We identified and analyzed 48 cases of IP theft that satisfied these criteria. We discovered the two dominant scenarios found within the cases (i.e., the Entitled Independent and Ambitious Leader Scenarios) only through extensive group discussion. These scenarios seemed to best make sense of the patterns we saw in the cases. However, other views into the nature of the problem are possible, and we invite other researchers to validate our insights or discover new aspects of the crime not previously observed. And we will continue to do the same.

The findings from case study comparisons in general, and our study in particular, cannot be generalized with any degree of confidence to a larger universe of cases of the same class or category. What this

method can provide, however, is an understanding of the contextual factors that surround and influence the event. The primary purpose of our modeling effort is precisely that – to help people understand the complex nature of the threat. Our models evolved through a series of group data analysis sessions with individuals experienced in both the behavioral and technical aspects of insider crimes. We used system dynamics, a method for modeling and analyzing the holistic behavior of complex problems as they evolve over time [24]. System dynamics provides particularly useful insight into difficult management situations in which the best efforts to solve a problem actually make it worse.

System dynamics model boundaries are drawn so that all the variables necessary to generate and understand problematic behavior are contained within them. This approach encourages the inclusion of soft (as well as hard) factors in the model, such as policy-related, procedural, administrator, or cultural factors. In system dynamics models, arrows represent the pair-wise influence of the variable at the source of the arrow on the variable at the target end of the arrow. A solid arrow indicates that the values of the variables move in the same direction, whereas a dashed arrow indicates that they move in the opposite direction.

A powerful tenet of system dynamics is that the dynamic complexity of problematic behavior is captured by the underlying feedback structure of that behavior. System dynamics models identify two types of feedback loops: balancing and reinforcing. Significant feedback loops are indicated in the model using a loop label appearing in parentheses in the middle of the loop. Reinforcing loops (indicated by a label with an R followed by a number) describe system aspects that tend to drive variable values consistently upward or downward and are often typified by escalating problematic behaviors. Balancing loops – (indicated by a label with a B followed by a number) tend to drive variables to some goal state and are often typified by aspects that control problematic behaviors. For those with color copies of the paper, loops are additionally distinguished by color, where black arrows are not part of a significant feedback loop.

4 The Entitled Independent Model

This section describes the system dynamics model of the Entitled Independent, an insider acting primarily alone to steal information to take to a new job or to his own side business.

4.1 Entitlement

The degree to which insiders felt entitled to information they stole is difficult to quantify without group interview data. However, interviews in a number of cases, along with the finding that 60% of this class of insiders stole information that they had at least partially developed or for which they had signed an IP agreement supports this hypothesis. Three-fourths of the Entitled Independents stole information in their area of responsibility, and 37% were at least partially involved with the development of the information stolen. 41% of the Entitled Independents stole information or products despite having signed IP agreements with the organization.

Figure 1 shows the escalation of entitlement to information developed by the insider. As shown in the upper right hand corner, an employee comes into an organization with a desire to contribute to its efforts. As the insider invests time in developing or creating information or products, his contribution to the organization becomes tangible. Such an individual, unlike his coworkers, has personal predispositions that result in a sense of entitlement to the information created by the group. This entitlement is shown in the self-reinforcing loop shown in purple and labeled R1 in the figure.

This sense of entitlement can be particularly acute if the insider perceives his role in the development of products as especially important. If the insider's work is focused on the contribution to a particular

product, for example a commercial software package, or the development of specific business information like customer contact lists, he may have a great sense of ownership of that product or information. This leads to an even greater sense of entitlement. This self-reinforcing loop is shown in blue and labeled R2. In addition, consistent with good management practice, individuals may receive positive feedback for their efforts, which they may interpret as particularly reinforcing, given their predispositions. In a recent insider case, one of the authors encountered a subject at significant insider risk who had been told his efforts had saved the company "millions of dollars." This compliment had the unintended consequence of reinforcing the entitlement loop.

Evidence of entitlement was extreme in a few cases. One Entitled Independent, who had stolen and marketed a copy of his employer's critical software, created a lengthy manuscript detailing his innocence and declaring that everyone at the trial had lied. After being denied a raise, another insider stole the company's client database and threatened to put them out of business on his way out the door.

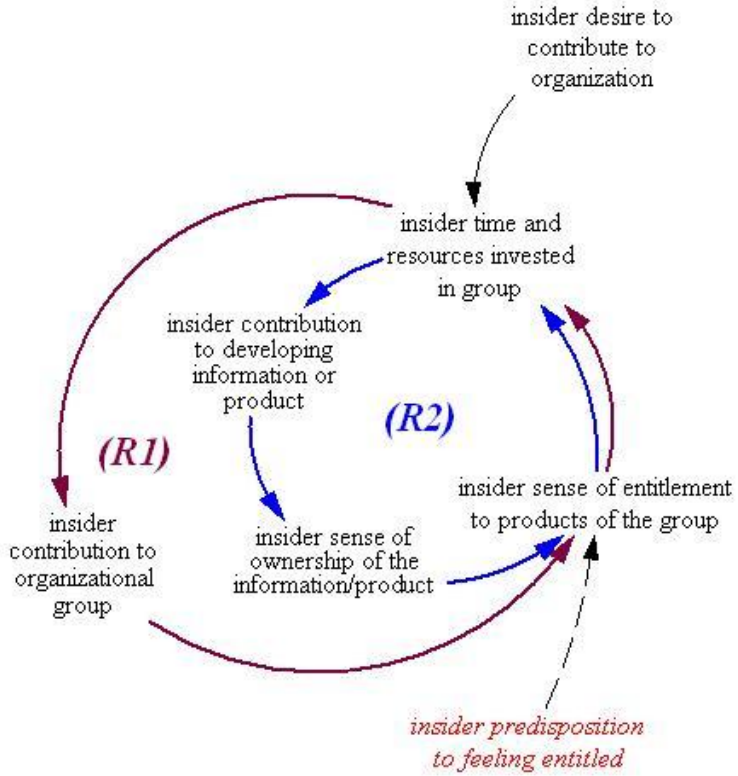


Figure 1: Insider Entitlement

4.2 Dissatisfaction Leading to Compromise

Expressed dissatisfaction played a role in 33% of the Entitled Independent cases. Dissatisfaction typically resulted from the denial of an insider's request, as shown in Figure2. Such denied requests in the cases studied often involved raises and benefits, applications for promotion, and requests for relocation. Dissatisfaction also resulted from the threat of layoffs within the victim organization.

The middle of Figure 2 shows that the organization's denial of an insider's request leads to the insider's dissatisfaction, which in turn decreases the insider's desire to contribute. This also affects the insider's ultimate sense of loyalty to the organization. Dissatisfaction often spurred the insider to look for

another job. Once the insider receives a job offer and begins planning to go to a competing organization, his desire to steal information increases. This desire is amplified by his dissatisfaction with his current employer and his sense of entitlement to the products developed by his group. In a third of the cases, the insider used the information to get a new job or to benefit his new employer in some way. In over a third of the cases (37%), the insider took the information just in case he ever needed it, with no specific plans in mind. One insider actually broke in after he was terminated to find out whether the organization had made any further progress on the product he had helped develop while he worked there.

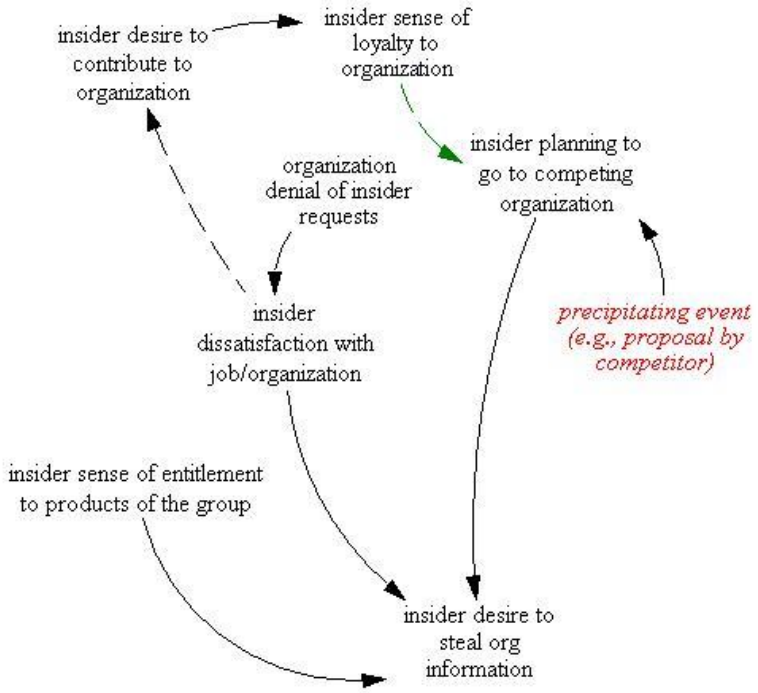


Figure 2: Insider Dissatisfaction Leading to Compromise

4.3 Theft and Deception

The insider's plan to go to a competing organization, dissatisfaction with his job and/or the organization, and his sense of entitlement to the products on which he has been working all contribute to the decision to steal the information. As shown in Figure 3, eventually the desire to steal information becomes strong enough, leading to the theft and the opportunity for the organization to detect the theft. Such opportunities arise when an organization observes an employee's actions, or consequences of those actions, that seem suspicious in some way. We discuss some of these opportunities later in this section.

Concern over being caught may make the insider think twice about stealing the information, as shown in the balancing loop labeled B1. Because our data consists of insiders who were caught and prosecuted, we do not know how many subjects may be deterred from insider acts by such concerns. However, our Entitled Independents did not exhibit great concern with being caught. This lack of concern is consistent with, and may be proportional to, the psychological predispositions that contribute to entitlement. Such individuals tend to overestimate their abilities and underestimate the capabilities of others. Despite IP agreements being in place in 41% of the cases, less than a quarter of the Entitled Independents explicitly attempted to deceive the organization while taking information.

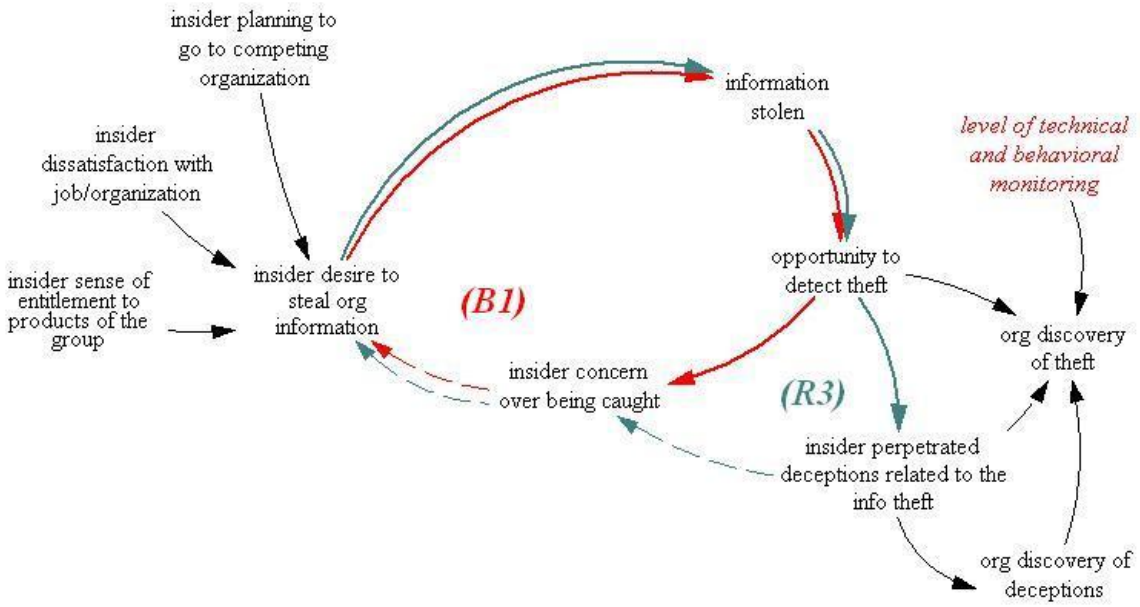


Figure 3: Insider Theft and Deception

Nevertheless, explicit deception can lessen the insider's concern over being caught, and should be anticipated by a vigilant organization. This is shown in the self-reinforcing loop labeled R3. This loop expresses the relationship between an insider's concern over being caught and deceptions committed that would embolden his theft of information. The fact that most insiders did not often feel it necessary to explicitly deceive the organization regarding the theft is interesting, suggesting the sense of entitlement, and its correlates mentioned above, may be particularly strong in these cases.

While explicit deception is not a major factor in this class of crimes, the fact that it does occur needs to be recognized. For example, upon announcing his resignation, one insider lied to his manager about having no follow-on employment, even though he had told a coworker about his new job at a competitor. As shown in the lower right part of Figure 3, deception may be an indicator of problems to come. Deceptions generally make it harder for the organization to sense the risk of theft and that is why the insider engages in such behavior. But if the organization is vigilant, deceptions may be discovered, alerting the organization to increased risk of insider threat. If the organization in the example had detected the contradictory information provided by the insider, it may have been forewarned of the heightened risk. In general, the organization's accurate understanding of its risk is directly related to its ability to detect the insider's actions. With sufficient levels of technical and behavioral monitoring these actions may be discoverable. Over half (52%) of the Entitled Independents stole information within one month of resignation, which gives organizations a window of opportunity for discovering the theft prior to employee termination.

4.4 Summary

Twenty-seven of the cases involved insiders acting as an Entitled Independent. AppendixB shows the final model of the Entitled Independent. In summary, well over half of the insiders who stole proprietary information appeared to feel entitled to that information, based on their theft despite signing an IP agreement or direct participation in the development of the stolen information. This sense of entitlement, when viewed in light of an event seen as dissatisfying to the insider, formed the catalyst for the insider

to begin looking for other jobs. Insiders then used stolen information to pursue new opportunities. The Entitled Independent is more often than not fully authorized for access to this information and steals it very close to resignation with very little planning. In addition, Entitled Independents infrequently act as if they are doing anything wrong, probably because they feel perfectly entitled to take the information or product with them to their new job.

5 The Ambitious Leader Model

This section describes the Ambitious Leader model. As noted, these cases involve a leader who recruits insiders to steal information for some larger purpose. The cases can be distinguished according to whether the insider

- had specific plans to develop a competing product or use the information to attract clients away from the victim organization (52%)
- was working with a competing organization to help his new employer (38%)
- sold the information to a competing organization (10%).

It also describes cases in which the insider was partially motivated by a desire to contribute to a foreign government or company (we view this as an implicit recruitment of insider help). The rest of this section describes additional aspects of the Ambitious Leader model not exhibited by Entitled Independents. This scenario is more complex than the Entitled Independent scenario, involving more intricate planning, deceptive attempts to gain increased access, and recruitment of other employees into the leader's scheme.

The motivation for the Ambitious Leader model is almost exactly the same as the Entitled Independent model described above. The primary difference, however, is that there was little evidence of employee dissatisfaction in the Ambitious Leader class (10%), whereas it played a more significant role with Entitled Independents (33%). Insiders in this scenario were motivated not by dissatisfaction but rather by an Ambitious Leader promising them greater rewards. In one case, the head of the public finance department of a securities firm organized his employees to collect documents to take to a competitor. Over one weekend he then sent a resignation letter for himself and each recruit to the head of the sales department. The entire group of employees started work with the competitor the following week. In another case, an outsider who was operating a fictitious company recruited an employee looking for a new job to send him reams of his current employer's proprietary information by email, postal service, and a commercial carrier.

Except for the dissatisfaction of the Entitled Independent, the initial patterns for Ambitious Leaders are exactly the same. In fact, the beginning of the Ambitious Leader model is merely the model shown in Appendix B without the "Insider Dissatisfaction with Job/Organization" variable shown in the middle left of the model. Theft took place even though IP agreements were in place for about half (48%) of the Ambitious Leader cases. In at least one case, the insider lied when specifically asked if he had returned all proprietary information and software to the company as stipulated in the IP agreement he had signed. He later used the stolen software to develop and market a competing product in a foreign country. Most (86%) of the insiders in the Ambitious Leader cases stole information or products in their area of job responsibility, with over half (62%) at least partially involved in developing the information or product stolen.

5.1 Insider Planning of Theft

The Ambitious Leader cases involved a significantly greater amount of planning than the Entitled Independent cases, particularly the recruitment of other insiders. Other forms of planning involved

- creating a new business (43%)
- coordinating with a competing organization (43%)
- collecting information in advance of the theft (38%)

This aspect of the insider behavior is reflected in the balancing loop labeled B2 in Figure4. The B2 loop parallels the loop B1 from the Entitled Independent model in Figure3 but describes an additional dimension: the insider's plans to steal information prior to the actual theft. This potential additional point of exposure of the impending theft includes the extensive planning described above and measures by the insider to hide his actions. Most of the Ambitious Leader cases involved planning by the insider a month or more before the insider's departure from the organization (71%). In almost half of the cases, the actual theft took place a month or more before the insider's departure (43%). One insider planned with a competing organization abroad and transferred documents to the company for almost two years prior to her resignation.

Forty-three percent of the insiders used deception to hide their plans for the theft of IP. The self-reinforcing loop labeled R3 is twice as strong for Ambitious Leaders than for Entitled Independents. In almost half of the cases (48%), the organization had IP agreements with the insiders explicitly stating the organization's ownership of the stolen information. In fact, there were only a few cases in which an IP agreement was in place between the organization and the insider but no deception was committed by the insider. This provides a working hypothesis regarding the effectiveness of an organization's efforts to promote its concern about IP theft. If the organizations involved publicized its concern and pursued violations, this may have increased the odds of deception while providing another observable indicator of insider risk.

5.2 Increasing Access

The amount of planning by the Ambitious Leader and insider subordinates he has recruited appears to depend on the extent to which any one participant has access to all of the information targeted for theft. The more segregation of privilege, the more planning, participation, and coordination are needed to commit the theft. In over half (52%) of the Ambitious Leader cases, the lead insider had authorization for only part of the information targeted and had to take steps to gain additional access. In the case involving the transfer of proprietary documents to a foreign company, the lead insider asked her supervisor to assign her to a special project that would increase her access to highly sensitive information. She did this just weeks prior to leaving the country with a company laptop and numerous company documents, both physical and electronic.

As shown on the right side of Figure 5, the recruitment of additional insiders is a primary means Ambitious Leaders use to gain access to more information. The need for recruitment increases the amount of planning activity necessary to coordinate insider activities. As shown in the self-reinforcing loop labeled R4 in Figure 5, as the insider invests more time and resources into the plans for theft and movement to the competing organization, it is less and less likely that they will back out of those plans.

While we can't know for sure that the R4 loop's self-reinforcement of insider criminal behavior is what is happening in these cases, there is strong evidence in the psychological literature for the "sunk cost effect." [25] The sunk cost effect involves an irreversible investment, e.g., time spent planning a theft

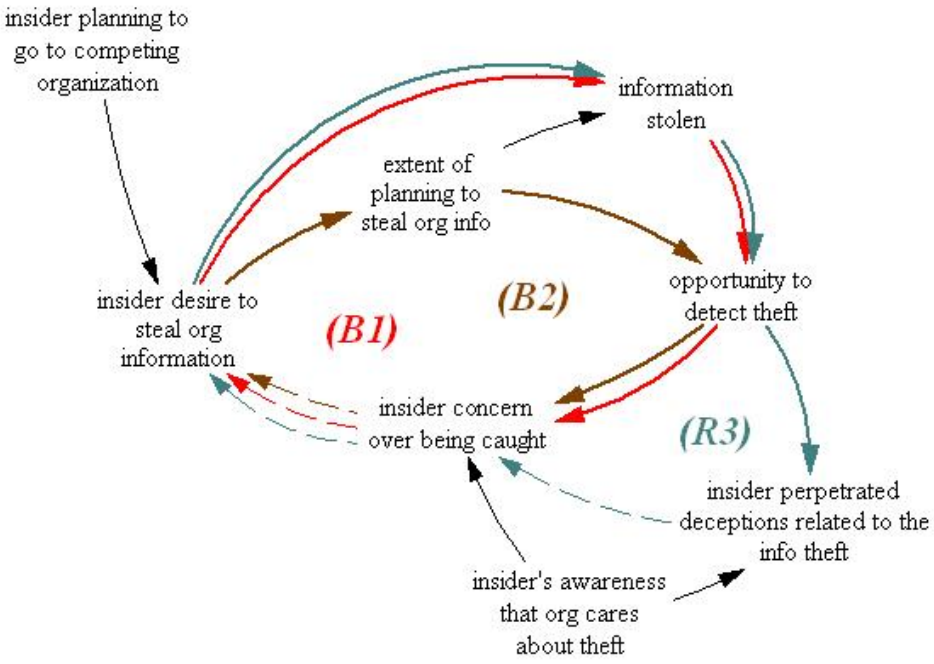


Figure 4: Theft Planning by Ambitious Leader

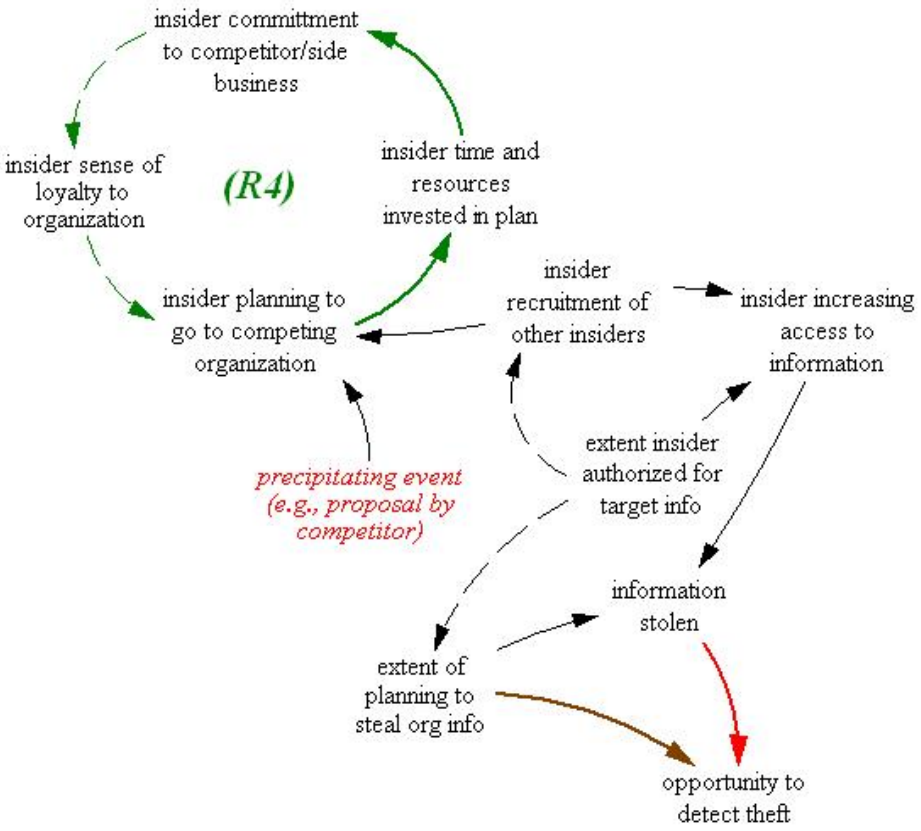


Figure 5: Increasing Access by the Ambitious Leader

that decision-makers consider as powerful motivation to continue the action. The further investment is justified not in terms of the initial rationale but because so much has already been invested [26].

There is evidence of this self-reinforcing pattern in one case of a job-hunting insider who met someone online who falsely claimed to own a competing business. While the insider was at first reluctant to send proprietary information, as the "friendship" grew and requests for confidential information repeated, the insider seemed unable to stop herself from gradually sending more and more of her employer's confidential information to the outsider. This indicates that insiders may be reluctant to back out of the plans because others are depending on them to carry out their part of the crime, not the least of which is the Ambitious Leader. At this point in the endeavor, the recruited insider is also subject to the same sanctions as the internal Ambitious Leader if their actions are discovered. In addition, the insider recruited by the Ambitious Leader outside the organization is also subject to blackmail once they have participated in the theft. The social costs of withdrawal from the scheme may therefore be too high, thus further motivating insiders to continue their involvement, even if they know it is wrong and would like to back out.

5.3 Organization Discovery of Theft

There are many more avenues for an organization to detect heightened risk of insider theft of IP in Ambitious Leader cases than in Entitled Independent cases. Entitled Independents are often fully authorized to access the information they steal, and do so very close to resignation with very little planning. In addition, Entitled Independents infrequently act as if they are doing anything wrong, probably because they feel a proprietary attachment to the information or product. Ambitious Leaders, on the other hand, often have to gain access to information for which they are not authorized. This involves, in part, coordinating the activities of other insiders and committing deception to cover up the extensive planning required.

Figure 6 illustrates the avenues available for an organization to continually assess the risk they face regarding theft of IP. The bottom of the figure shows the discovery of insider deception. Because deception is such a prominent factor in Ambitious Leader cases, its discovery may be a better means to detect heightened insider risk here than in Entitled Independent cases.

In some of the cases we reviewed, the organization found out about the theft because the insider tried to use the information. Two primary uses were observed: marketing of the competing product to the general public or to the victim organization's customers, and soliciting the business of the victim organization's customers. While these two uses are not extremely different, they do differ based on what was stolen – in the first case, the organization's product (e.g., software system) and, in the second case, client information (e.g., organization business plans or client points of contact). In one case, the insider had stolen source code for a product being marketed by his previous employer and was demonstrating a slightly modified version at a trade show. Unfortunately for him, his previous co-workers observed the activity and alerted the authorities. While this detection is later than one would prefer, it is still not too late to take action and prevent further losses.

Organizations could use technical monitoring systems to achieve earlier detection of insider plans or actions to steal IP. Over half (52%) of the Entitled Independents and almost two-thirds (62%) of the Ambitious Leader insiders stole information within one month of resignation. Many of these involved large downloads of information outside the patterns of normal behavior by those employees. In over a quarter (29%) of the Ambitious Leader cases, an insider emailed or otherwise electronically transmitted information or plans from an organizational computer. Keeping track of backup tapes is also important – in the case described in the previous paragraph, the insider took the backup tape from his computer on his last day of work. Understanding the potential relevance of these types of precursors provides a window of opportunity for organizations to detect theft prior to employee termination.

Of course, the earlier an organization can become aware of such plans the better. Early awareness depends on behavioral as well as technical monitoring and is more likely to catch incidents involving

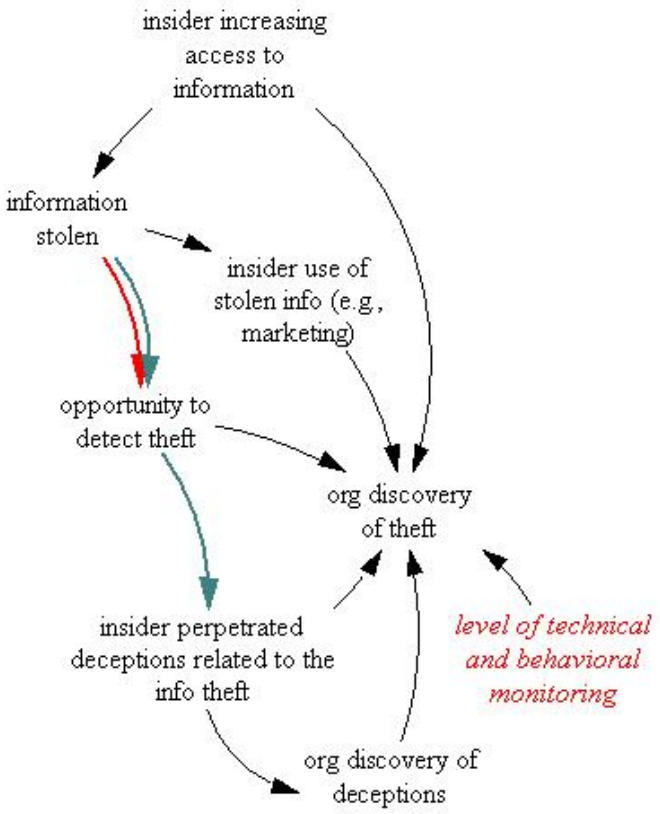


Figure 6: Organization Discovery of Theft of IP in Ambitious Leader Cases

Ambitious Leaders than Entitled Independents. In Ambitious Leader scenarios, the organization needs to look for evolving plans and collusion by insiders to steal information, including attempts to gain access to information over and above that for which an employee is authorized. There were behavioral or technical precursors to the crime in all of the Ambitious Leader cases. One insider, over a period of several years, exhibited suspicious patterns of foreign travel and remote access to organizational systems while claiming medical sick leave. It is not always this blatant, but signs are often observable if an organization is vigilant.

5.4 Insider IP Theft Benefiting a Foreign Entity

Twelve of the 48 cases of IP theft (25%) were intended to benefit a foreign government or company. All of these cases fit the model of the Ambitious Leader scenario and were included in the statistics reported in this section. In these cases, loyalty to their native country trumped loyalty to the employer. Similar to the way insiders in the other cases were motivated by an Ambitious Leader, insiders with an affinity toward a foreign country were motivated by the goal of bringing value to, and sometimes eventually relocating in, that country. In all of the Ambitious Leader cases, there is an influencing individual and motive acting on the subject to promote the criminal act.

5.5 Summary

Twenty-one of the 48 cases involved Ambitious Leaders acting as the insider or guiding the insider to steal information. The final model of the Ambitious Leader is shown in Appendix C. Ambitious

Leader cases involved more planning and deception than Entitled Independent cases, as there was more coordination necessary between insiders and greater understanding of the impropriety involved. This combined with the fact that at least some of the theft often occurred within a month of the insider's departure means there were many chances for an organization to detect the heightened risk of Ambitious Leader attacks. In some cases, the Ambitious Leader was an agent of a foreign interest, and the theft of information was geared toward the benefit of a foreign entity.

6 Conclusion

This paper describes two models of insider theft of IP. Section 4 presents the model of the Entitled Independent. Section 5 presents the model of the Ambitious Leader. While these two models overlap significantly, the Ambitious Leader Model – which extends the Entitled Independent Model - has more potential indicators for early warning. Together these two models present the big picture of insider theft of IP and, though preliminary, form our essential contribution.

These models were developed using empirical data from cases involving actual insider compromise. The primary frequencies derived from our analysis are given in Figure 7. The hypotheses derived from the analysis are:

- Entitled Independents often show signs of job dissatisfaction.
- Insiders who steal IP almost always steal information within area of their job responsibility and are usually at least partially involved with the development of that information. Entitled Independents are more likely to exhibit this property than are Ambitious Leaders.
- Ambitious Leaders engage in a significant amount of planning of the theft of IP.
- Ambitious Leaders often start stealing information more than a month prior to their departure from the organization.
- Insiders who steal IP usually steal at least some of the information within a month of their resignation.
- Ambitious Leaders often engage in explicit deceptions concurrently with committing their crime.
- Insiders who steal IP are more likely to engage in explicit deceptions when they have previously signed an IP agreement.
- Insiders who steal IP are more likely to recruit other insiders if they need information outside of their job responsibility.
- As insiders invest more time and resources into the planning the theft, it is less and less likely that they will back out of those plans.

This work has focused on gaining a more rigorous understanding of the nature of the threat and providing an effective means for communicating that to the general public. We have found that the system dynamics approach helped to structure and focus the team's discussion. This was particularly important since members of the team, by necessity, came from the different disciplines of psychology and information security. The models also provided a concrete target for validation through mapping to observables exhibited by the real-world cases.

Of course, this is only the beginning of the work. Future work needs to further validate the hypotheses embodied in the model. Model validation will occur only incrementally as we and other researchers study

the theft of IP class of crimes to substantiate (or refute) the hypotheses generated in our study. Further model validation will likely require richer data than we had available to us in this study. In addition, our ultimate concern is to develop effective measures to counter the problem of theft of IP. Significant methodological and data challenges must be overcome before research on insider activity can be soundly prescriptive for mitigation policies, practices, and technology. However, we cannot overestimate the importance of looking at the total context of adverse insider behavior for understanding why these events happened and how they might be prevented in the future.

	Entitled Independent	Ambitious Leader	Overall
signs of job dissatisfaction	33%	10%	23%
disregarded IP agreement	41%	48%	44%
planning more than one month before departure	33%	71%	50%
stole within area of job responsibility	74%	86%	79%
at least partially developed information stolen	37%	62%	48%
started stealing more than one month before departure	19%	43%	29%
stole within one month of resignation	52%	62%	56%
explicit deception	22%	43%	31%

Figure 7: Key Aspects of Insider Theft of IP Cases

By using the system dynamics approach we will attempt to assess the weight and interrelatedness of personal, organizational, social, and technical factors. We expect future work to use modeling and simulation to identify and evaluate the effectiveness of deterrent measures in the workplace, such as those suggested in [27]. Experiments such as those conducted at Mitre can also help validate hypotheses about the problem and test deterrent measures [22]. Prospective studies of these phenomena will always be challenging because of low base rates. In the meantime, system dynamics modeling and experimental studies based on available empirical data can bridge this methodological gap and translate the best available data into implications for policies, practices, and technologies to mitigate insider threat.

7 Acknowledgments

CERT would like to thank the Army Research Office and Carnegie Mellon University's CyLab for funding this project. Our original insider threat work was funded by the U.S. Secret Service whose support we will always be grateful for. We would also like to thank the following for their contributions to our insider threat efforts and this project: Daniel Phelps of Carnegie Mellon University; Christopher Nguyen

and Hannah Joseph, former CERT employees while students at the Information Networking Institute of Carnegie Mellon University; Michael Hanley and Greg Longo, employees of CERT; and Ed Desautels, technical editor of the SEI.

References

[1] E. Rich, I. Martinez-Moyano, S. Conrad, D. Cappelli, A. Moore, and T. S. et.al., "Simulating insider cyber-threat risks: A model-based case and a case-based model," in *Proc. of the 23rd International Conference of the System Dynamics Society , Boston, USA*. System Dynamics Society, July 2005.

[2] D. Capelli, L. Fischer, A. Moore, E. Shaw, and R. Trzeciak, "Common sense guide to prevention and detection of insider threat (3rd ed.)," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep., September 2008.

[3] J. Predd, S. Pfleeger, J. Hunker, and C. Bulford, "Insiders behaving badly," *IEEE Security and Privacy*, vol. 6, no. 4, pp. 66–70, July/August 2008.

[4] P. Sackett, "The structure of counterproductive work behaviors: Dimensionality and relationships with facets of job performance," *International Journal of Selection and Assessment*, vol. 10, pp. 5–11, 2002.

[5] P. Sackett and C. Devore, "Counterproductive behaviors at work," in *Handbook of Industrial, Work and Organizational Psychology*, N. Anderson, D. Ones, H. Sinangil, and C. Viswesvaran, Eds. New York, NY: Sage Publications, Ltd., 2001, pp. 145–164.

[6] D. Anderson, D. Cappelli, J. Gonzalez, M. Mojahedzdeh, A. Moore, E. Rich, and et.al., "Preliminary system dynamics maps of the insider cyber-threat problem," in *Proc. of the 22nd International Conference of the System Dynamics Society, Keble College, Oxford, UK*. System Dynamics Society, July 2004.

[7] A. Moore, D. Cappelli, and R. Trzeciak, "The 'big picture' of insider it sabotage across U.S. Critical Infrastructures," in *Insider Attack and Cyber Security: Beyond the Hacker*, S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, and S. Smith, Eds. New York, NY: Springer Science+Business Media, LLC, 2008, pp. 17–52.

[8] D. Cappelli, A. Desai, A. Moore, T. Shimeall, E. Weaver, and B. Willke, "Management and education of the risk of insider threat (MERIT): Mitigating the risk of sabotage to employers' information, systems, or networks," in *Proc. of the 24th International Conference of the System Dynamics Society, Nijmegen, The Netherlands*. System Dynamics Society, July 2006.

[9] J. Salgado, "The big five personality dimensions and counterproductive behaviors," *International Journal of Selection and Assessment*, vol. 10, pp. 117–125, 2002.

[10] M. Mount, R. Ilies, and E. Johnson, "Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction," *Personnel Psychology*, vol. 59, pp. 591–622, 2006.

[11] C. Stamper and S. Masterson, "Insider or outsider? how employee perceptions of insider status affect their work behavior," *Journal of Organizational Behavior*, vol. 23, no. 8, pp. 875–894.

[12] D. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley and Sons, 1998.

[13] B. Wood, "An insider threat model for adversary simulation," in *Proc. for Research on Mitigating the Insider Threat to Information Systems*. The RAND Corporation, August 2000.

[14] J. Suler and W. Phillips, "The bad boys of cyberspace: Deviant behavior in multimedia chat communities," *CyberPsychology and Behavior*, vol. 1, pp. 275–294, 1998.

[15] E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," *Security Awareness Bulletin*, no. 2-98, pp. 27–46, 1998.

[16] E. Spafford, "A framework for understanding and predicting insider attacks," *Computers and Security*, vol. 21, no. 6, pp. 526–531, October 2002.

[17] T. Gudaitis, "The missing link in information security: Three dimensional profiling," *Cyber Psychology and Behavior*, vol. 1, no. 4, pp. 321–340, 1998.

[18] S. Band, D. Cappelli, L. Fischer, A. Moore, E. Shaw, and R. Trzeciak, "Comparing insider IT sabotage and espionage: A model-based analysis," Software Engineering Institute, Carnegie Mellon University, Pittsburgh,

PA, Tech. Rep. CMU/SEI-2006-TR-026, December 2006.

[19] L. Fischer, "Characterizing information systems insider offenders," in *Proc. of the 45th Annual Conference of the International Military Testing Association (IMTA'03), Jason Cope, UK*, 2003.

[20] K. Herbig and M. Wiskoff, "Espionage against the United States by American citizens 1947-2001," Defense Personnel Security Research Center, Monterrey, CA, Tech. Rep. PERSEREC-TR-02-5, July 2002.

[21] E. Shaw and L. Fischer, "Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders," Defense Personnel Security Research Center, Monterrey, CA, Tech. Rep. PERSEREC-TR-05-13, September 2005.

[22] D. Caputo, G. Stephens, and M. Maloof, "Detecting insider theft of trade secrets," *IEEE Security and Privacy*, vol. 7, no. 6, pp. 14–21, November/December 2009.

[23] R. Yin, *Case Study Research (4th ed.)*. Thousand Oaks, CA: Sage Publications, 2009.

[24] J. D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*. New York, NY: McGraw-Hill, 2000.

[25] M. Sastry, "Analyzing the research on self reinforcing processes in organizations: Another approach to archetypes," in *Proc. of the 16th International Conference of the System Dynamics Society, Quebec City, Canada*. System Dynamics Society, July 1998.

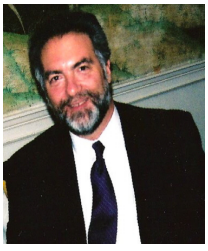
[26] B. Staw and J. Ross, "Understanding behavior in escalation situations," *Science*, vol. 246, no. 4927, pp. 216–220.

[27] M. McCormick, "Data theft: A prototypical insider threat," in *Insider Attack and Cyber Security: Beyond the Hacker*, S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, and S. Smith, Eds. New York, NY: Springer Science+Business Media, LLC, 2008, pp. 53–68.

Andrew P. Moore is a senior member of the CERT technical staff. Moore explores ways to improve the security, survivability, and resiliency of enterprise systems through insider threat and defense modeling, incident processing and analysis, and architecture engineering and analysis. Before joining the SEI in 2000, he worked for the Naval Research Laboratory (NRL) investigating high-assurance system development methods for the Navy. He has over twenty years experience developing and applying mission-critical system analysis methods and tools, leading to the transfer of critical technology to both industry and the military. Moore received his BA in Mathematics from the College of Wooster and MA in Computer Science from Duke University.

Dawn Cappelli, CISSP, is Technical Manager of CERT's Enterprise Threat and Vulnerability Management Team at Carnegie Mellon University's Software Engineering Institute. Her team's mission is to assist organizations in improving their security posture and incident response capability by researching technical threat areas; developing information security assessment methods and techniques; and providing information, solutions and training for preventing, detecting, and responding to illicit activity. Team members are domain experts in insider threat and incident response. Team capabilities include threat analysis and modeling; development of security metrics and assessment methodologies; and creation and delivery of training and workshops. Dawn has 30 years experience in software engineering, including programming, technical project management, information security, and research. She is often an invited speaker at national and international venues, is adjunct professor in Carnegie Mellon's Heinz College of Public Policy and Management and currently Vice-Chair for the CERT Computer Security Incident Handler Certification Advisory Board. Before joining CMU in 1988 she worked for Westinghouse as a software engineer developing nuclear power systems.

Tom Caron is a Senior Consultant at Deloitte Consulting, where he specializes in IT security and enterprise software training. He advises on web application portals, enterprise resource planning implementation, people-based IT security issues, and regulatory compliance initiatives. He has deep experience in the field of system documentation tools and has provided solutions across the energy, consumer business, health care, communications, publishing, manufacturing, media, aerospace and defense, and state government industry sectors. His research interests lie at the intersection of people and security issues. Tom holds a Bachelor of Science in Business Administration with a Concentration in Management Information Systems from Boston University and a Master of Science in Information Security Policy and Management from Carnegie Mellon University.



Eric Shaw is a Clinical Psychologist and former intelligence officer who has spent the last ten years performing consultations, assisting in investigations and conducting research on insider issues while helping organizations manage insider risk. He specializes in psychological profiling of insider risk using multiple methods, including content analysis of subject communications. Dr. Shaw has served as a Visiting Scientist at the Software Engineering Institute where he assists CERT in understanding the individual, social and organizational psychology associated with insider risk and computer crime. He is also currently performing test-bed validation on a patented content analysis system designed to detect signs of insider risk from computerized communications. He was recently selected by the Department of Justice to serve as an expert witness on insider issues involved in litigation resulting from the Anthrax attacks in 2001. Dr. Shaw's publications on insider challenges and the role of behavioral science and profiling in forensic and security issues have appeared in Digital Investigation,

Information Security Magazine, Security Management, The Police Chief and Studies in Conflict and Terrorism. In addition to his consulting practice, Dr. Shaw is a Professorial Lecturer in Political Psychology at the Elliot School of International Studies of George Washington University and maintains a private clinical practice in Washington, D.C. He is certified in critical incident stress debriefing and served with the FBI's Evidence Recovery Teams at the Pentagon after the September 11th attacks. He received his B.A. from Colgate University and his Masters and Ph.D. in Psychology from Duke University. He performed a fellowship in Psychology in the Department of Psychiatry at the Payne Whitney Clinic of New York Hospital–Cornell University Medical Center and subsequently served on the faculty.

Derrick Spooner is currently an Information Security Analyst at CERT. He is a critical member of the insider threat center which focuses on insider threat research, threat analysis and modeling, assessments, and training. He holds an MS in Information Security Policy Management from Carnegie Mellon University and a BA in Information Technology Leadership from Washington & Jefferson College.

Randy Trzeciak is currently a senior member of the technical staff at CERT. He is the technical team lead of the Insider Threat Outreach and Transition group in the Insider Threat Center at CERT; a team focusing on insider threat research; threat analysis and modeling; assessments; and training. Randy has over 20 years experience in software engineering, database design, development, and maintenance, project management, and information security. Before joining Carnegie Mellon University, Randy worked for Software Technology Incorporated, in Alexandria VA, as a consultant to the Naval Research Laboratory (NRL). He also is an adjunct professor at Carnegie Mellon's Heinz College, School of Information Systems and Management. Randy holds an MS in Management from the University of Maryland and a BS in Management Information Systems and a BA in Business Administration from Geneva College. Prior to his current role at CERT, Trzeciak managed the Management Information Systems team in the Information Technology Department at the Software Engineering Institute (SEI). Prior to working at the SEI, Trzeciak was a software engineer at the Carnegie Mellon Research Institute. Previously he was a lead developer and database administrator at Computing Services at Carnegie Mellon. Prior to his career at Carnegie Mellon, Trzeciak worked for Software Technology, Inc. in Alexandria, Virginia. He holds an MS in Management from the University of Maryland and a BS in Management Information Systems and a BA in Business Administration from Geneva College.

A Nature of Insider Theft of Intellectual Property Crimes

Who were the insiders?

- 92% of the insiders who stole IP were male (males comprise 78% of CERT's overall case repository where gender is known).
- 56% held technical positions (technical positions comprised 48% of the overall case repository where positions were known).
- 75% were current employees when they committed their illicit activity (current employees comprise 74% of CERT's case repository where employment status is known).
- 65% of the insiders had already accepted positions with another company or had started a competing company at the time of the theft.

Why did they do it?

- 35% of the insiders stole the information to gain an immediate advantage at a new job.
- In 25% of the cases, the insider gave the information to a foreign company or government organization. The average financial impact for cases involving the benefit for a foreign entity was over four times that of domestic IP theft.

When did the attacks happen?

- 78% of the crimes were committed during working hours when the time of theft was known (26% of CERT's overall cases were committed during work hours).
- 56% stole within a month of their departure from the organization (this characteristic drops to 9% when viewed across all crimes in the CERT repository).
- Less than one third of the insiders continued their theft for more than one month; and of those that did so, roughly one quarter of them stole the information for a side business, and roughly three quarters to take to a new employer.

How did they attack?

- Almost three-quarters of the insiders had authorized access to the information stolen at the time of the theft. (31% of the insiders across all crimes had authorized access at the time of the theft).
- None of the insiders had privileged access (such as that given to a system or database administrator), which enabled them to commit the crime (8% of all crimes involved an insider with privileged access).
- In approximately 19% of the cases, the insider colluded with at least one other insider to commit the crime (insiders collaborated with accomplices 24% of the time overall).
- The insider was actively recruited by someone outside the organization in 25% of the cases.
- 65% of the insiders attacked at the workplace; only 15% attacked remotely, accessing their employers' networks from their homes or from another organization. In 25% of the cases the location of the attack was unknown.

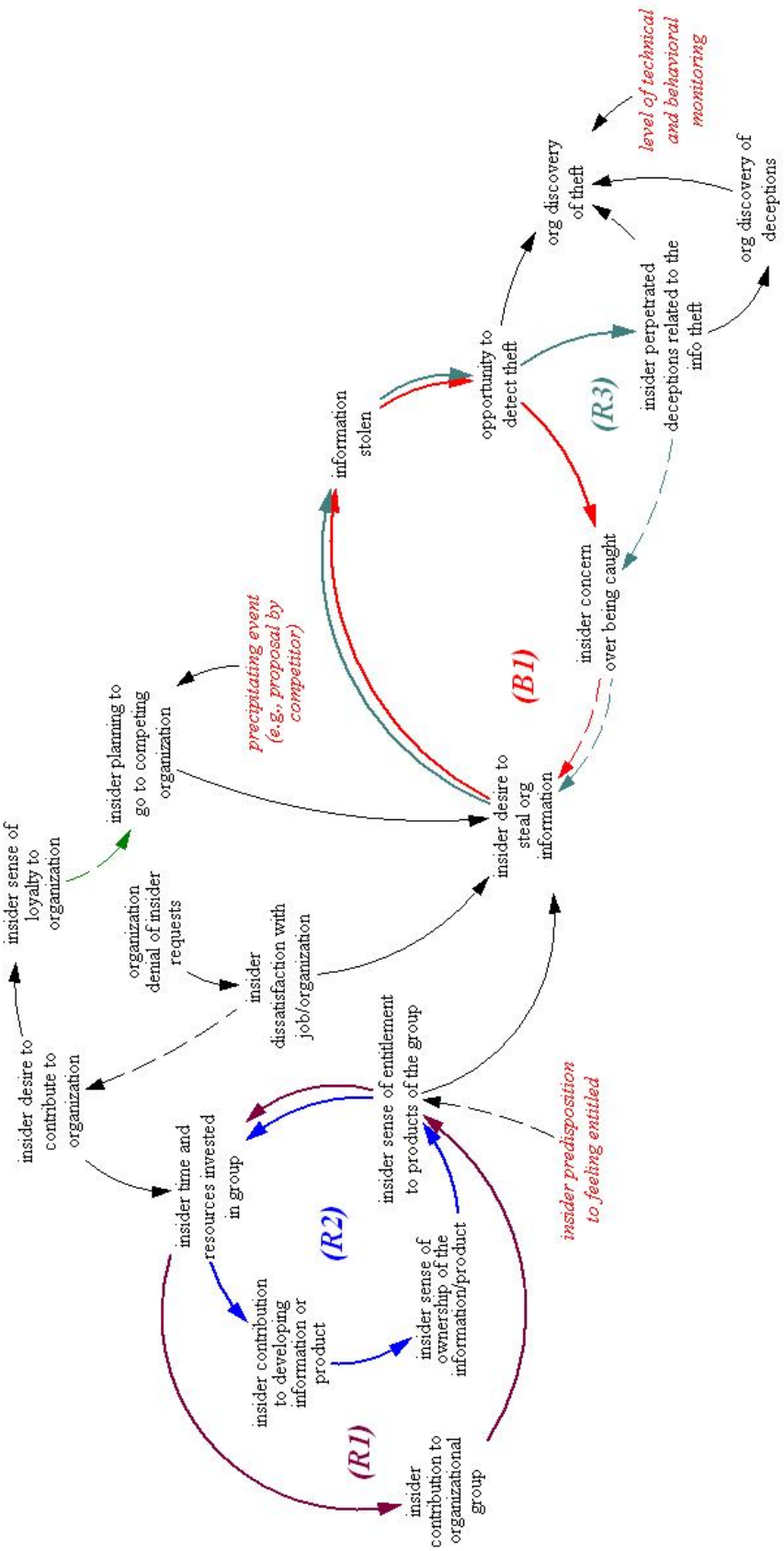
How was the theft detected?

- Many of these incidents were detected by non-technical means: for example, notification by a customer or other informant, detection by law enforcement investigating the reports of the theft by victims, reporting of suspicious activity by co-workers, and sudden emergence of new competing organizations.
- The most likely person to discover an insider theft is a non-technical employee. In cases where we were able to isolate the person who discovered the incident, 72% were detected by non-technical employees (non-technical employees were responsible for discovering insider crime in 11% of the overall case repository).

What were the impacts?

- In 31% of the cases, proprietary software or source code was stolen (insiders targeted software in 10% of the entire CERT case repository).
- 17% of cases involved business plans, proposals, and other strategic plans (insiders targeted business plans in 4% of the entire CERT case repository).
- 31% involved product information, such as product designs or formulas (trade secrets were stolen in 7% of the cases in CERT's repository, regardless of crime type).
- 15% involved customer lists or customer data (This information was targeted 29% of the time across all crimes).
- 10% involved the organization's physical property (physical property was the target in 6% of CERT's cases overall).

B Entitled Independent Model for Insider IP Theft



C Ambitious Leader Model for Insider IP Theft