Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model*

Andrew P. Moore apm@cert.org, Dawn M. Cappelli dmc@cert.org,
Thomas C. Caron[1] tcaron@cert.org, Eric Shaw[2] eshaw@msn.com,
Randall F. Trzeciak rft@cert.org

CERT®[3] Program, Software Engineering Institute and
CyLab at Carnegie Mellon University
4555 Fifth Avenue
Pittsburgh, PA 15213

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 35 cases of insider theft of intellectual property. In the context of this paper, insider theft of intellectual property for business advantage includes incidents in which the insider's primary goal is stealing confidential or proprietary information from the organization with the intent to use it to take to a new job, to get a new job, or to start a business. It does not include cases of in which insiders sell an organization's information. 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 mititgative measures in future work.

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 IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to the critical infrastructure of the United

* This paper appears in the proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST 2009), Purdue University, West Lafayette, 15-19 June 2009.

[1] Tom Caron is also a student at the H. John Heinz III College, School of Information Systems Management, Carnegie Mellon University.

[2] Dr. Eric Shaw is a Visiting Scientist at CERT and clinical psychologist at Consulting & Clinical Psychology, Ltd.

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

States.4 Consequences of malicious insider incidents include financial losses, operational impacts, damage to reputation, and harm to individuals. The actions of a single 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.

Many models exist to help understand computer-related malicious insider activity, including

- the Capability, Motive, Opportunity Model (Parker, 1998) (Wood, 2002)
- behavioural models (Suler, 1997) (Shaw, Ruby, & Post, 1998)
- an entity relationship model in a comprehensive characterization framework[5] (Spafford, 2002)
- a criminological and social model (Gudaitis, 1998)

The Defense Personnel Security Research Center (PERSEREC) has produced a vast amount of invaluable data over the years on both espionage and insider threat. (Fischer, 2003) (Herbig & Wiskoff, 2002) In one article, a multiple case study approach was used to examine 10 cases of malicious insider IT activity in critical infrastructures drawn from the population of PERSEREC cases. (Shaw & Fischer, 2005) In addition, the Institute for Information Infrastructure Protection (I3P) has brought a wide range of researchers in industry and government to bear on the insider threat problem. [6]

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 organization—especially the unintended consequences of policies, practices, technology, efforts to manage insider risk, and organizational culture over time.[7] As part of MERIT, we have been using system dynamics modelling and simulation to better understand and communicate the threat to an organization's information technology (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 has evolved into the Security Dynamics Network and the Security Special Interest Group (Anderson, et al., July 2004).

---

[4] "Insiders" include current and former employees, contractors, or other business partners who have or had authorized access to their organization's systems, data, and networks. Insiders are familiar with internal policies, procedures, and technology and can exploit that knowledge to facilitate attacks and even collude with external attackers.

[5] Unpublished manuscript: Tuglular and Spafford, "A Framework for Characterization of Insider Computer Misuse.

[6] See http://www.thei3p.org/research/insider_threat.html.

[7] CERT's insider threat research is published on http://www.cert.org/insider_threat. Early research was funded by the U.S. Secret Service and the Department of Homeland Security, Office of Science and Technology. Our current work including MERIT was funded by Carnegie Mellon University CyLab.

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 mititgative measures. CERT has found four categories of insider threat cases based on the patterns we have seen in cases identified: IT sabotage, theft or modification of information for financial gain (fraud), theft of intellectual property (IP) for business advantage, 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 for business advantage. Our past work has involved modeling insider fraud (Rich, et al., July 2005), insider IT sabotage (Moore, Cappelli, & Trzeciak, 2008)(Cappelli, Desai, Moore, Shimeall, Weaver, & Willke, July 2006), and espionage (Band, Cappelli, Fischer, Moore, Shaw, & Trzeciak, December 2006).

We define insider theft of IP for business advantage 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 and used it to get another job, help a new employer, or promote their own side business. Cases in which the insider was primarily motivated by personal financial gain have significantly different patterns of behavior and have been excluded from this study (Cappelli, Moore, Trzeciak, & Shimeall, September 2008). While an argument can be made that theft of confidential or proprietary information may ultimately be about money, insiders in this class of cases generally had longer term ambitions, such as stealing the information to get a new job, to succeed in a new job with a competing business, to start a competing business, or to give the stolen data to a foreign government or organization.

This paper is centered on two dominant scenarios found within the cases: the Entitled Independent Scenario and the Ambitious Leader Scenario. 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 for business advantage. 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 Approach

Our research approach is based on the comparative case study methodology (Yin, 2003). The cases we selected fit the above definition of theft of IP for business advantage. 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 35 cases of IP theft that satisfied these criteria. 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 sole 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. 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 a 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 blue arrows are not part of a significant feedback loop.

3 The Entitled Independent Model

This section describes the system dynamics model of the Entitled Independent, an ambitious insider acting alone to steal information to take to a new job or to his own side business. Note that in most cases (80%) the insider had no specific plans to use the information.

3.1 Entitlement

The degree to which insiders felt entitled to information they stole is difficult to quantify without group interview data. However, feedback from a small sample of subjects, along with the finding that many insiders stole information from their project area despite having signed IP agreements, supports this observation. Almost all of the Entitled Independents stole information in their area of responsibility, and about half were at least partially involved with the development of the information stolen. Just over 44% of the Entitled Independents stole information or products despite having signed IP agreements with the organization. The strong sense of entitlement is seen in this class of insiders when considering that nearly 75 percent of the insiders stole information that they had at least partially developed or for which they had signed an IP agreement.

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 (yellow loop). 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 yellow 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.

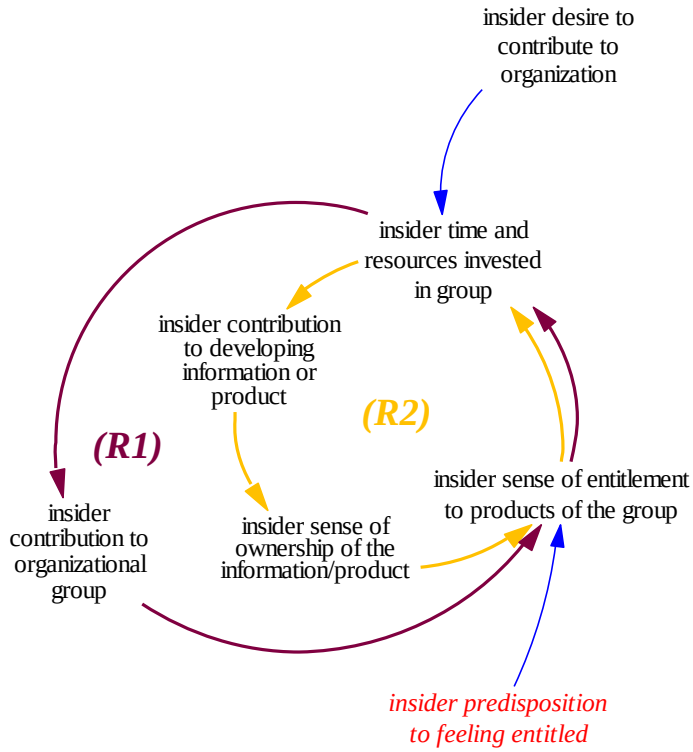


Fig. 1. Insider Entitlement

3.2 Dissatisfaction Leading to Compromise

Expressed dissatisfaction played a role in 39% of the Entitled Independent cases. Dissatisfaction typically resulted from the denial of an insder's request, as shown in Figure 2. 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 amplified his dissatisfaction with his current employer in combination with his sense of entitlement to the products developed by his group. In a third of the cases (33%), the insider used the information to get a new job or to benefit his new employer in some way. In almost half of the cases (44%), 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.

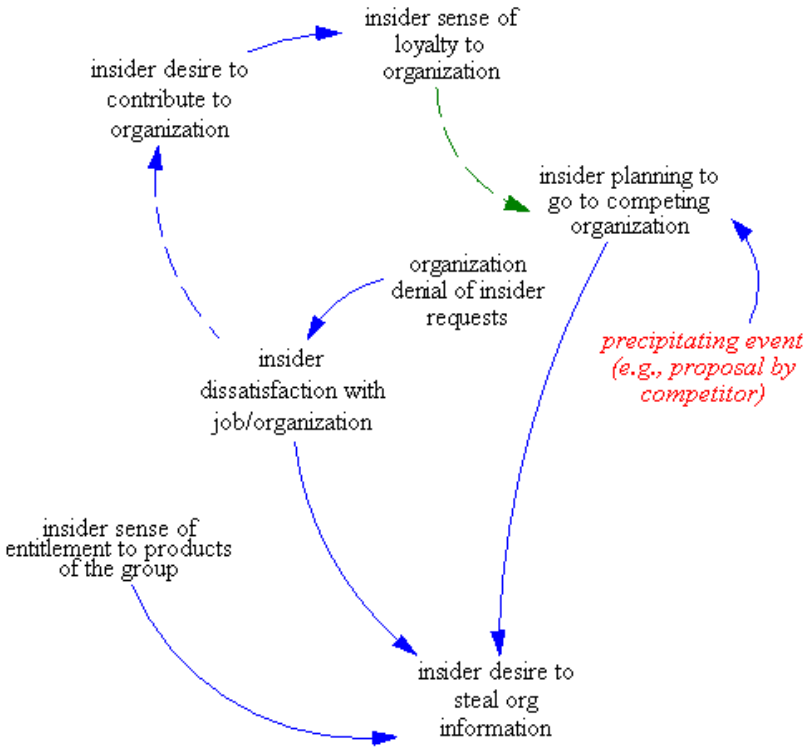


Fig. 2. Insider Dissatisfaction Leading to Compromise

3.3 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 44% of the cases, less than a quarter of the Entitled Independents explicitly attempted to deceive the organization while taking information.

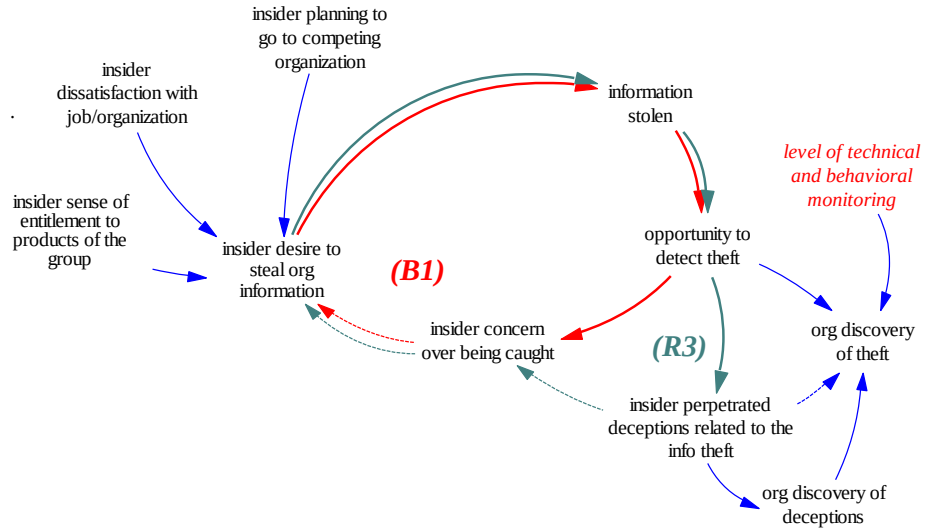


Fig. 3. Insider Theft and Deception

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 being provided by the insider, it may have predicted an attempt to steal its IP. In

general, the organization's accurate understanding of its risk is directly related to its ability to detect the insider's actions, which, with sufficient levels of technical and behavioral monitoring, may be discoverable. Over half (56%) 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.

3.4 Summary

Appendix B shows the final model of the Entitled Independent. Based on the patterns observed in the cases, half of the insiders who stole proprietary information felt a sense of entitlement to that information, based on their participation in its development, regardless of whether or not they signed an IP agreement. 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 usually fully authorized for access to this information and steals it very close to resignation with very little planning. In addition, Entitled Independents rarely acts 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.

4 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 (60%)
- was working with a competing organization to help his new employer (40%).

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 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 and deception attempts to gain increased access, and recruitment of other employee's 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 (6%), whereas it played a more significant role with Entitled Independents (39%). 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 (46%) 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. Almost all of the insiders in the Ambitious Leader cases stole information or products in their area of job responsibility, with over half of those at least partially involved in developing the information or product stolen. These facts strongly suggest that the insiders felt a sense of entitlement to the information or products that they stole.

4.1 Insider Planning of Theft

The Ambitious Leader cases involved a significantly greater amount of planning than the Entitled Independent cases. By definition, the cases involved recruiting of insiders which necessitates a greater amount of planning. Other forms of planning involved

- creating a new business (37%)
- coordination with a competing organization (37%)
- collecting information in advance of the theft (60%)

This aspect of the insider behavior is reflected in the balancing loop labeled B2 in Figure 5. The B2 loop parallels the loop B1 from the Entitled Independent model in Figure 4 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 (84%). 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.

About a third (34%) of the insiders used deception to hide their plans for the theft of IP. The self-reinforcing loop labeled R3 is slightly stronger in this case than for the Entitled Independent. In all but one of these cases, the organization had IP agreements with the insiders explicitly stating the organization's ownership of the stolen

information. In fact, there was only one case 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.

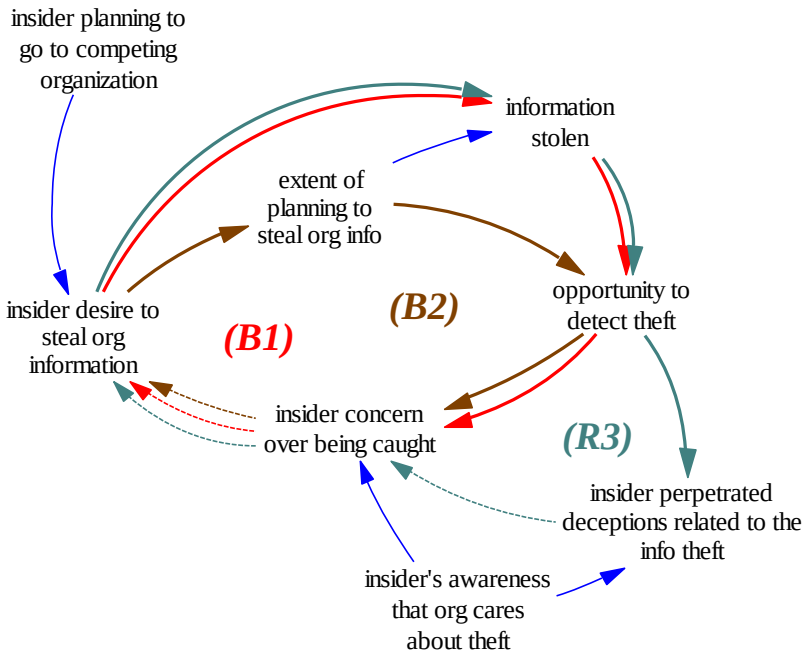


Fig. 4. Theft Planning by Ambitious Leader

4.2 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 (55%) 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. This is in stark contrast to the Entitled Independent cases where two-thirds (67%) of the primary insiders were authorized to access all of the information stolen.

As shown on the right side of Figure 6, 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.

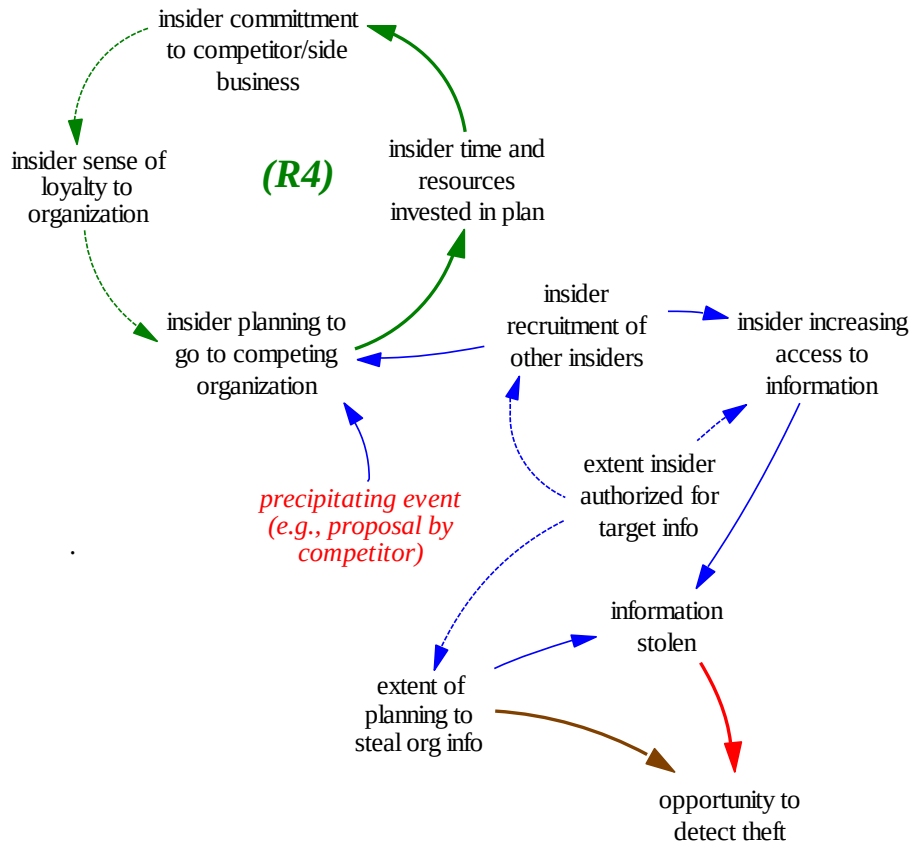


Fig. 5. Increasing Access by the Ambitious Leader

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." (Sastry, 1998) The sunk cost effect involves an irreversible investment (e.g., time spent planning a theft) 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 (Staw & Ross, 1989).

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. The social costs of withdrawal from the scheme may be too high, thus further motivating insiders to continue their involvement, even if they know it is wrong and would like to back out.

4.3 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 usually fully authorized to access the information they steal, and do so very close to resignation with very little planning. In addition, Entitled Independents rarely acts 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 7 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 to steal, or actual theft, of IP.. Over half (56%) of the Entitled Independents and almost two-thirds (67%) 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 one-third (38%) 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.

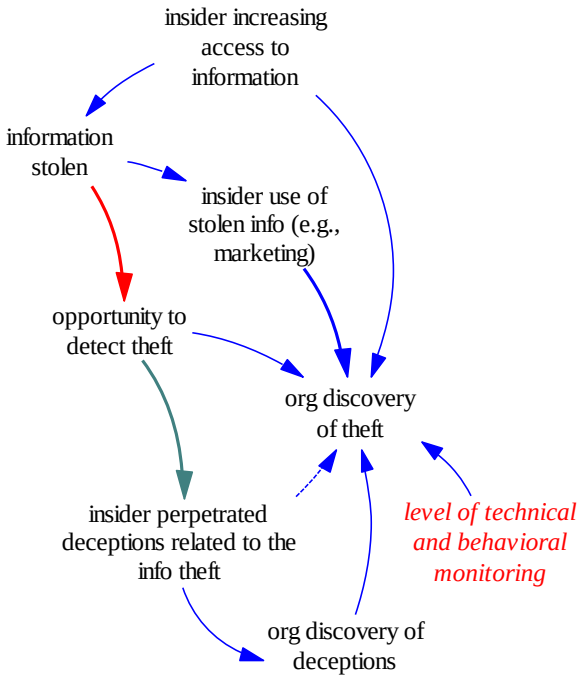


Fig. 6. Organization Discovery of Theft of IP in Ambitious Leader Cases

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 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. Such attempts occurred in over 2/3 (69%) of the 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.

4.4 Insider IP Theft Benefiting a Foreign Entity

Nine of the 35 cases (26%) of IP theft 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.

4.5 Summary

While half of the cases involved insiders acting as Entitled Individuals, the other half were characterized by 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 much more planning and deception, as insiders typically did not initially have access to the data in question. These attacks were more likely to occur closer to the point at which the insider left the organization. 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.

5 Conclusion

This paper describes two models of insider theft of IP for business advantage. They were developed using empirical data from cases involving actual insider compromise. The following key observations describe the overarching patterns in the cases of insider theft of IP.

- Many insiders exhibited a sense of entitlement to the information they stole. Insiders generally disregarded IP agreements (44%).
- Many Entitled Independents showed signs of dissatisfaction with some aspect of their job, often compensation, benefits, or promotions (39%). No insiders stealing for the benefit of a foreign government or company showed signs of dissatisfaction.
- The insiders were evenly split according to whether they had authorized access to only part or all of the information stolen. The majority of Entitled Independents had authorized access to the information they stole (67%). The majority of Ambitious Leaders did not have authorized access to all of the information they stole (69%).
- Most insiders were involved with significant planning activities more than a month before resignation. (59%).
- Some insiders started stealing information more than one month prior to their departure. (21%).
- Most insiders stole at least some information within a month of resignation (65%).
- Most insiders stole information in their area of job responsibility (74%), and many at least partially developed the information and/or product stolen (41%).

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. 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.

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. Prospective studies of these phenomena will always be challenging because of low base rates. In the meantime, system dynamics modeling using 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.

6 Acknowledgements

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 CERT; Christopher Nguyen and Hannah Joseph, former CyLab employees and graduates of the Information Networking Institute of Carnegie Mellon University; Michael Hanley and Greg Longo, current CERT employees and students of the Heinz College of Carnegie Mellon University.

This paper appears in the proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST 2009), Purdue University, West Lafayette, June 15-19, 2009.

7 Bibliography

Anderson, D. F., Cappelli, D. M., Gonzalez, J. J., Mojahedzadeh, M., Moore, A. P., Rich, E., et al. (July 2004). Preliminary System Dynamics Maps of the Insider Cyber-

Threat Problem. *Proceedings of the 22nd International Conference of the System Dynamics Society.*

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (December 2006). *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis.* Carnegie Mellon University, Software Engineering Institute.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J. (July 2006). Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks. *Proceedings of the 24th International System Dynamics Conference.* Nijmegen, Netherlands.

Cappelli, D. M., Moore, A. P., Trzeciak, R. F., & Shimeall, T. J. (September 2008). *Common Sense Guide to Prevention and Detection of Insider Threat* (3rd ed.). CERT Program, Software Engineering Institute, and CyLab of Carnegie Mellon.

Fischer, L. (2003). *Characterizing Information Systems Insider Offenders.* Pensacola, FL: International Military Testing Association Proceedings.

Gudaitis, T. (1998). *The missing link in information security: Three Dimensional Profiling"* (Vol. 1). Cyber Psychology and Behavior.

Herbig, K. L., & Wiskoff, M. (2002). *Espionage Against the United States by American Citizens 1947-2001.* Defense Personnel Security Research Center.

Meadows, D. L., Behrens, W. W., Meadows, D. H., Naill, R. F., Randers, J., & Zahn, E. K. (1974). *Dynamics of Growth in a Finite World.* Cambridge, MA: Wright Allen Press, Inc.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures* (Vol. Insider Attack and Cyber Secruity: Beyond the Hacker). (S. Stolfo, S. M. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, & S. W. Smith, Eds.) New York, NY: Springer Science+Business Media, LLC.

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information.* New York: John Wiley and Sons.

Rich, E., Martinez-Moyano, I. J., Conrad, S., Cappelli, D. M., Moore, A. P., Shimeall, T. J., et al. (July 2005). Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model. *Proceedings of the 16th International Conference of the System Dynamics Society.* Quebec City, Canada.

Sastry, M. A. (1998). Analyzing the research on self reinforcing processes in organization: Another approach to archetypes. *Proceedings of the 16th International Conference of the System Dynamics Society.* Quebec City, Canada.

Shaw, E., & Fischer, L. G. (2005). *Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders.* Defense Technical Information Center.

Shaw, E., Ruby, K. G., & Post, J. M. (1998). *The Insider Threat to Information Systems: The Psychology of the Dangerous Insider* (Vols. 2-98). Security Awareness Bulletin.

Spafford, E. (2002). *A Framework for Understanding and Predicting Insider Attacks* (Vol. COMPSEC 2002). London: Elsevier Science Ltd.

Staw, B. M., & Ross, J. (1989). Understanding Behavior in Escalation Situations. *Science* , *246*, 216-220.

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

Suler, J. (1997). *The Bad Boys of Cyberspace: Deviant Behaviour in On-Line Multimedia Communities and Strategies for Managing It.* http://www.rider.edu/~suler/psycyber/badboys.html.

Wood, B. (2002). *An Insider Threat Model for Adversary Simulation.* RAND.

Yin, R. K. (2003). *Case Study Research.* (3rd, Ed.) Thousand Oaks: Sage Publications.

Appendix A: Nature of Insider IP Theft for Business Advantage

Who were the insiders?	• 91% of the insiders who stole IP were male (males comprise 82% of CERT's overall case repository where gender is known). • 55% held technical positions (technical positions comprised 56% of the overall case repository where positions were known). • 65% were current employees when they committed their illicit activity (current employees comprise 70% of CERT's case repository where employment status is known). • Nearly 80% 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?	• 32 % of the insiders stole the information to gain an immediate advantage at a new job. • In 21% 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?	• 73% of the crimes where information was available were committed during working hours (37% of CERT's overall cases were committed during work hours). • 37% stole within a month of their departure from the organization (this characteristic drops to 7% 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, half of them stole the information for a side business, and half to take to a new employer.
How did they attack?	• Over three-quarters of the insiders had authorized access to the information stolen at the time of the theft. (27% of the insiders across all crimes had authorized access at the time of the theft). • None of the insiders had privileged access[8], which enabled them to commit the crime (6% of all crimes involved an insider with privileged access). • In approximately 15% of the cases, the insider colluded with at least one other insider to commit the crime (insiders collaborated with accomplices 22% of the time overall). • The insider was only actively recruited by someone outside the organization in less than 25% of the cases. • 68% of the insider attacked at the workplace (21% attacked

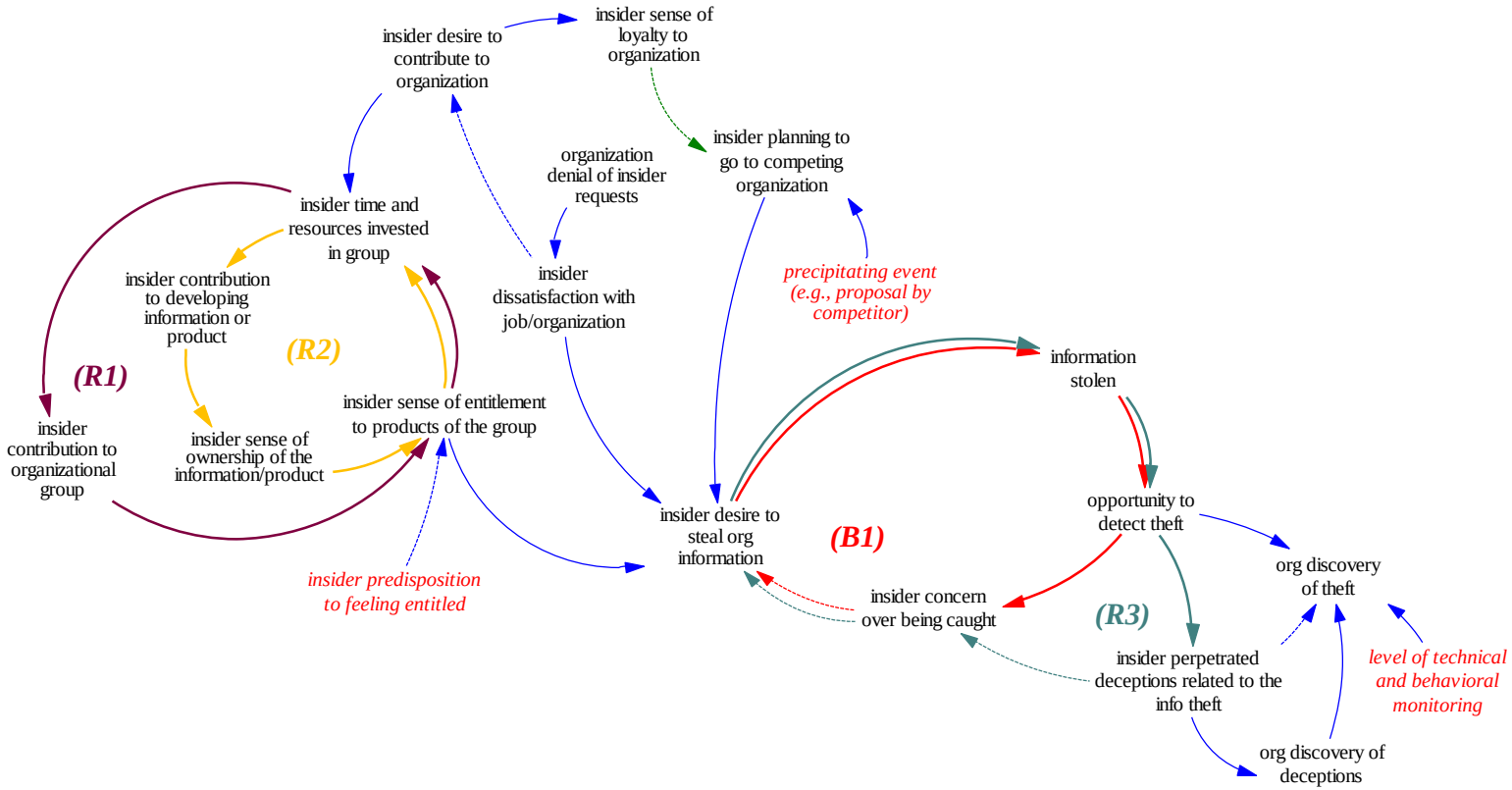
[8] Such as that given to a system or database administrator.

	remotely, accessing their employers' networks from their homes or from another organization. In 11% 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, such as:
	  ○ 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 for business advantage is a non-technical employee. In cases where we were able to isolate the person who discovered the incident, 57% were detected by non-technical employees (non-technical employees were responsible for discovering insider crime in 36% of the overall case repository).

What were the impacts?	• In 26% of the cases, proprietary software or source code was stolen (insiders targeted software in 8% of the entire CERT case repository). • 29% of cases involved business plans, proposals, and other strategic plans (insiders targeted business plans in 5% of the entire CERT case repository). • 63% involved trade secrets, such as product designs or formulas (trade secrets were stolen in 15% of the cases in CERT's repository, regardless of crime type). • 20% involved customer lists or customer data (This information was targeted 23% of the time across all crimes). • 20% involved the organization's physical property (physical property was the target in 8% of CERT's cases overall).

Appendix A: Entitled Independent Model for Insider IP Theft



Appendix B: Ambitious Leader Model for Insider IP Theft