System Dynamics Based Insider Threats Modeling

Sang-Chin Yang [1] and Yi-Lu Wang [2]

[1] The Institute of Resource Management and Decision Science, Management College, National Defense University, Tahsi, Taoyuan 33509, Taiwan, Republic of China
jsreliability@gmail.com
[2] School of Defense Science, Chung Cheng Institute of Technology, National Defense University, Tahsi, Taoyuan 33509, Taiwan, Republic of China
ms6903@gmail.com

ABSTRACT

Insider threat has been recognized as one of the most dangerous security threats and become a much more complex issue. Insider threat is resulted from the legitimate users abusing their privileges and cause tremendous damage or losses. Not always being friends, insiders can be main threats to the organization. Currently, there is no equivalent prevention solution for insider threat to an intrution prevention system or vulnerability scanner. From the survey of literature of insider threat studies, we conclude that the system dynamics (SD) is an effective tool to analyze the root causes of insider threat incidents and evaluate mitigation strategies from people, process, and technology perspectives. A generized case based SD model can be tailored and applied to analyze and evaluate specific insider threat incidents. We present a well known insider threat incident of Taiwan and tailor the generized case based SD model to analyze it. The simulation results indicate that the risk of insider threats can be reduced and the probability of detecting insider threats can be increased.

KEYWORDS

System Dynamics, Insider Threat, Modeling

1. Introduction

Information technologies occupy a pivotal position in critical infrastructures protection, but they are changing due to innovate rapidly. The issue of information security is increasingly important for homeland security. According to the 2010 CyberSecurity Watch Survey [1] posits that multiple attacks can occur within larger organizations, and insiders remain the most costly threat. We know the greatest threat to information systems, such as important national defence and critical infrastructure, is often an insider threat. According to 67% of respondents, incidents of insider threats are more costly than outsider breaches. Researchers have been developing new approaches for making information systems more secure, offering advanced security strategies, frameworks, models, and assessment methods. However, most of those researches are focused on attacks from outside. Cybercrimes committed by insiders are often more costly and damaging than attacks from the outside. Insider threats result from legitimate users abusing their privileges, causing tremendous damage or losses. Insiders can be the main threats to an organization. Given the limited ability of existing systems to counter abnormal insider behaviours, many of the security technologies that have been studied only prevent threats from outsider attacks. This paper presents a case based system dynamics model to simulate and analyze insider behaviours. This paper also provides interactive simulation-based experiments to demonstrate the ability of the model to create insider behaviour profiles that accurately reflect the risks and mitigations involved in the insider threat problem, as well as the model's efficiency.

DOI : 10.5121/ijnsa.2011.3301

Insiders can be stopped, but stopping them is a complex problem [2]. Management must pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment to prevent insider theft through a layered defense strategy consisting of policies, procedures, and technical controls. Therefore, Organizations must look beyond information technology to their overall business processes and the interplay between those processes and the technologies used. Testimony from the U.S. Department of Homeland Security [3] asserts that the DHS S&T Cyber Security program must develop new ways to detect and mitigate insider threats in cyber security. Computer crime or cybercrime refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of the crime [4]. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. The threats posed by computer crime to many targeted organizations are increasing faster than they can combat them, according to the 2010 Cyber Security Watch Survey conducted by CSO magazine, the leading resource for security professionals, and sponsored by Deloitte's Center for Security and Privacy Solutions. Moreover, the survey suggests current security models, which are only minimally effective against cyber criminals, heighten the threat of cybercrime. The MERIT project [5] was initiated as a proof of concept – to determine whether or not an effective interactive learning environment could be developed to teach executives, managers, technical employee, human resources, and security officers the complex dynamics of the insider threat problem.

The structure of this paper is organized as follows. Section 2 provides an overview of the literature related to our work; we present our framework in Section 3 through the case of the well-known enterprise and related models, which we evaluate in the same section. Section 4 provides the system dynamics and simulation model of our contribution. Finally, Section 5 concludes the paper with an overview of our future research directions.

2. Related work

In the related work, we classify and arrange a brief summary of the research in insider threat analysis from 1999 to 2010. We have to separate people, process and technology in these articles and most of them focus on technology. Anderson proposes 8 general approaches to mitigate the insider threat [6], and Schultz presents a framework to understand and predict insider attacks [7]. Symonenko et al prove Natural Language Processing (NLP) system to integrate the results of social network analysis, role-based access monitoring, and semantic analysis of insiders' communications [8]. Liu and Martin investigate anomaly detection techniques [9]. Chinchani presents a theory of insider threat assessment. Stanton et al. analyze end user security behaviors [10]. Park and Giordano develop monitoring mechanisms based on role-level analysis and individual profiles [11]. Maybury summarizes and characterizes the automatic detection of malicious insiders within modern information systems [12]. Butts extends the Schematic Protection Model to produce the first comprehensive security model capable of analyzing the safety of a system against the insider threat [13]. Ha et al. demonstrate the feasibility of applying capability acquisition graphs to insider threat analysis [14]. Ali et al. present an Agent-based User-Profiling model that monitors the behavior of the authorized users in an organization to avoid risk [15]. McCormick assesses the threat of confidential data leakage, focusing on its most virulent form -- insider data theft attacks [16]. Chagarlamudi et al. present a model that can prevent malicious insider activities at the database application level [17]. Jabbour and Menasce present the Insider Threat Security Architecture (ITSA) and a security scenario where privileged users can compromise the system that they protect, and they discuss ways in which that same scenario can be mitigated under the ITSA framework [18].

Nellikar focuses on the advantages of using role based mechanisms for insider threat detection [19].

Anderson's paper "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems" addresses 4 categories for insider threat [20]. Bishop and Gates' article "Defining the Insider Threat" define an insider [21]; both of these models are classified as "process". Niekerk and Solms present a conceptual model to facilitate conceptual thinking and argumentation in the culture of information security [22].

However, we believe that all these studies have neglected a crucial element: people. Keeney, Cappelli, Band, Greitzer, and Moore et al. have all used system dynamics to prevent insider threat [23-28]. This method not only embraces technology, but also includes process and people. We arrange these references in Table 1, sorted by date of publication.

Table 1. Historical background of insider threat analyses and their attributes

Authors	Methodology	Classification
Anderson (1999)	4 categories of insider threat	Process
Anderson (2000)	8 general approaches	Technology
Schultz (2002)	6 indicator framework	Technology
Symonenko et al. (2004)	Natural Language Processing (NLP) system	Technology
Keeney et al. (2005)	MERIT	People/process/Technology
Liu and Martin (2005)	KNN outlier detection algorithm	Technology
Chinchani (2005)	Modeling methodology / threat assessment methodologies	Technology
Stanton et al. (2005)	End user security behaviors	Technology
Park and Giordano (2006)	Role-based Access Control	Technology
Maybury (2006)	Detecting algorithm of malicious insiders	Technology
Cappelli et al. (2006)	MERIT	People/process/Technology
Band et al. (2006)	System dynamics	People/process/Technology
Butts (2006)	SPM-IT / MAMIT approach	Technology
Cappelli, et al. (2006)	System dynamics	People/process/Technology
Ha et al. (2007)	ICMAP	Technology
Ali et al. (2008)	Crystal Report Generation	Technology
Bishop and Gates (2008)	Definition of an insider	Process
Greitzer et al. (2008)	MERIT	People/process/Technology
McCormick (2008)	Multi-pronged holistic EDLP program	Technology
Moore et al. (2008)	System dynamics	People/process/Technology
Chagarlamudi et al. (2009)	Implementation-oriented approach	Technology
Jabbour and Menasce (2009)	Insider Threat Security Architecture	Technology
Nellikar S (2010)	Scalable Simulation Framework	Technology
Niekerk and Solms (2010)	Conceptual model	Process

System dynamics begins with the work of Jay Wright Forrester. System dynamics is a computer-aided approach that can define problems dynamically and build confidence in the model. It applies interdependence, mutual interaction, information feedback, and circular causality to dynamic problems arising in complex social systems.

One of the fundamental principles of system dynamics is the hypothesis that a model predicts behavior, which is the key element in this article. The importance of the connection between model and behavior is easily seen in Forrester's introduction to Industrial Dynamics [29].

System dynamics models also can be stand-alone. It formulates the problem of representing behavior over time as the problems of distinguishing the key variables in the situation, graphing the behavior of those variables over time. The concept of System Dynamics is shown in Fig 1.

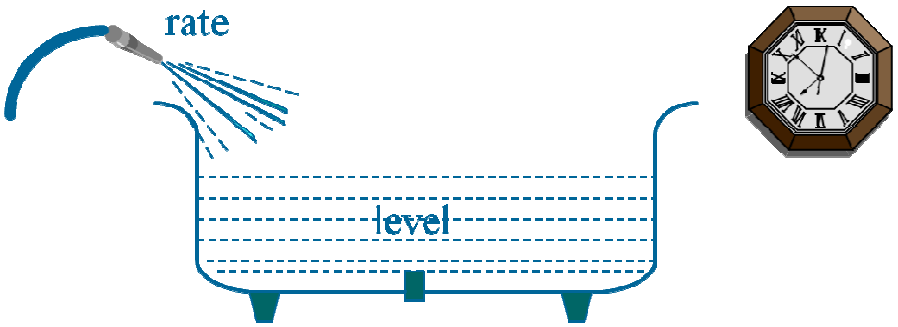


Figure 1. Metaphor of System Dynamics

The modeling principle is shown in Fig 2. System dynamics seeks to identify feedback mechanisms within a system to explain the system's behavior [30].

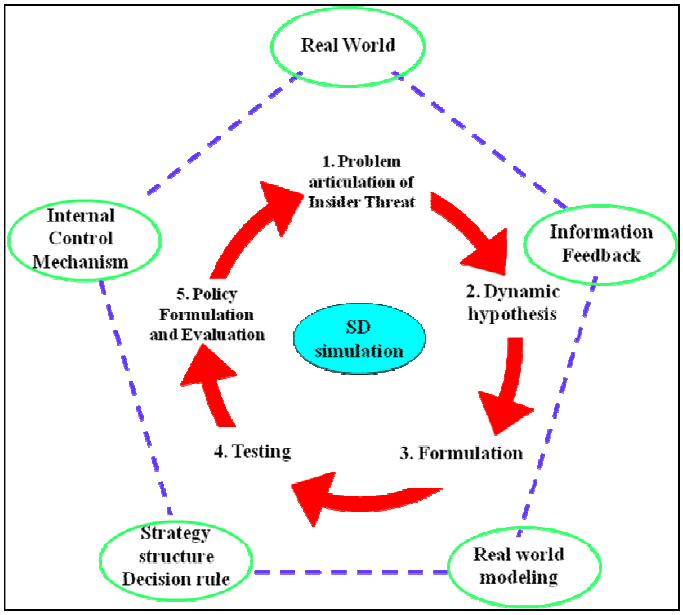


Figure 2. Modelling Principle of System Dynamics

In this article, we construct a tailored model that presents the prevention of insider threat in a well-known enterprise by means of a system dynamics and feedback learning perspective. These simple stochastic processes may not capture the complex real-world behavior of uncertainties that result from nonlinear feedback structures, such as rework and learning curves. Using system dynamics to model the structure that produces this complex behavior may improve the accuracy of the ultimate valuation. Another advantage of system dynamics methodology is its ability to define complex feedback systems and separate stochastic effects, which is quite beneficial in dealing with multiple and potentially interacting sources of uncertainty. The distribution of uncertainty around the system dynamics variables is intuitive, thanks to the methodology's emphasis on the use of concrete variables that correspond to "real" phenomena.

3. Case Study

For a background of system dynamics, we highlight one of Taiwan's biggest corporate theft cases, involving the unauthorized sale of 127.8 million shares owned by an American merchant that were under the control of a well-known enterprise. An insider spirited away NT$3.1 billion from the illegal sale of shares entrusted to the enterprise by a U.S. company which is an American merchant Corp. Employee A (insider, under judgment) is still missing. Investigators have also failed to track down Employee A's elder brother, who worked at a local trading firm, after Employee A left Taiwan on a forged passport. The investigators have not ruled out the possibility that Employee A's brother was aware of the astonishing financial scam from the beginning. He could even have been an accomplice, according to sources at the investigation bureau. Extraordinarily, both the brother and his wife have disappeared, although no records show they have left Taiwan. They could also have used false documents to escape, said the sources. There are reports that Employee A had used a novel scheme to purchase over 200 carats of expensive diamonds from various jewelry stores with payments transferred from his bank account in Hong Kong. Investigators said Employee A's father, who had been on the top 10 wanted list after escaping to the United States 10 years ago, could have been the mastermind pulling the strings behind the scenes. Employee A's father escaped to the United States 10 years ago after forging documents to raise excess loans from a well known state-run bank in Taiwan, where he was once a deputy manager. Employee A joins his father on the list of Taiwan's 10 most-wanted fugitives who have absconded abroad. There was no explanation for the discrepancy between the well-known enterprise's explanation and report. The enterprise had given American Merchant a cash payment of NT$678 million (US$20 million), the company said in a statement issued from its headquarters. The enterprise had also agreed to pay American merchant an additional NT$1.52 billion (US$45 million) over four years in 16 quarterly installments secured by letters of credit, it said. It had also given the American merchant a credit of NT$620 million (US$18.3 million) for future legal services. Furthermore, American merchant had agreed to donate to Taiwanese and US charities an unused amount of US$1 million in credits for legal services, to be paid annually for 18 years, displaying broad-mindedness on the part of a high-tech company and creativity on the part of the professional service company.

This represents cost-sharing between the two parties and exemplifies the common concern for a society that characterizes their corporate values. This sort of stakeholder-centered spirit is the best expression of the extended enterprise. In order to construct the system dynamics model, the time sequence of this incident is presented in Table 2. From the case statement given above and Table 2, we can deduce that because the well-known enterprise had inadequate insider audit procedures to disperse and control the risks, it accepted the risks of losing clients, employees' loyalty, and having a debt of NT$3.1 billion. It could easily have detect and prevent Employee A's crime if the bank had discharged its monitoring obligation acceptably.

When an insider threat occurs, it often has significant ramifications for the integral image and business operation of the industry. Fortunately, the enterprise in our case handled the subsequent situations well, and suffered no lasting effects. Nevertheless, damage will be minimized if it is possible to detect malicious motive and behavior at the outset, which is the primary purpose of this research. We shall construct a system dynamics model of this case. It is helpful to understand the malicious behavior pattern and take appropriate measures.

Table 2. Time-sequence table of an incident in a well-known enterprise

Time	Event
2002.02	An American merchant signs a contract to manage the stock sale of a well-known enterprise.
2002.05	Employee A asks his roommate to hand over his identification card, passport, certificate of registered residence, and order of retirement. Employee A's roommate acts accordingly.
2002.09	Employee A takes his own picture and pretends to be "Employee A's roommate". He professes that his identification card is lost, and asked the administration office to reissue it. Ten days later, he asks that his passport be reissued.
2003.07	Employee A goes to Hong Kong secretly and sets up the nominal "New Emperor Investment Company". Investigators later find that he had remitted money to the "New Emperor" account of the overseas department of the bank and that he set up an account related transaction of Asian negotiable securities without authorization.
2003.08	The American merchant remits 121 million shares to a contract account. Employee A sees the action signal appear, and on the same day, he asks for a one year unpaid leave of absence from October 1, in order to prepare for the special attorney examination. Employee A starts to sell this batch of stocks without authorization.
2003.09	As the retail stock contract was going to expire, the well-known enterprise wanted to collect the entire related stock transaction account item and returned the funds to the consignor. At this time, unexpectedly, all the funds from sale of stocks vanish into thin air. After an internal audit, the legal personnel who had stored the funds develop a suspicion, and he presents an indictment against Employee A .
2003.10	Employee A's unauthorized sale of NT$3.1 billion worth of stock of the American merchant company without authorization is detected by another employee of the well-known enterprise. The senior partner officially convenes the press conference and announces the theft and unauthorized sale

4. Simulation model

We use system dynamics to model the above incident for insider threat analysis. From the timetable, we can assume that the insider had the expected level of freedom, as in figure 3. We also know that lazy management unintentionally encouraged the escalation of expectations, as seen in the simulation results in Figure 4. The simulation starts off with the expectations and sense of achievement at an equal value of 10 on a scale of relative freedom. This is a rather arbitrary measure of the relative freedom allowed any employee of the organization according to the organization's appropriate systems usage policy. With a lazy management, some employees will try to "push the envelope," using the system as desired regardless of the organization's usage policy. This is especially true for insiders with a strong sense of entitlement. This simulation illustrates a situation in which lazy management permits increasing freedom to the insider, which can cause major problems later on, especially if that insider has a

predisposition towards disgruntlement. The trigger for those major problems, which we call the precipitating event, can be anything that removes or restricts the freedom to which the insider has become accustomed. In the well-known case in Taiwan case, as in some of the cases in the Insider Threat Study, the trigger is loss of Partner status.

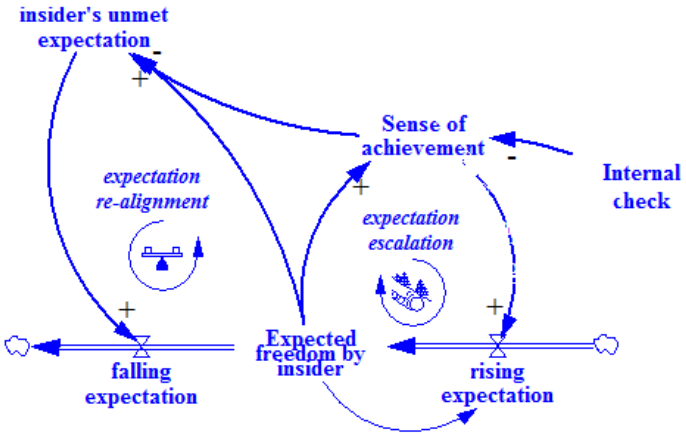


Figure 3. Expected freedom by insider

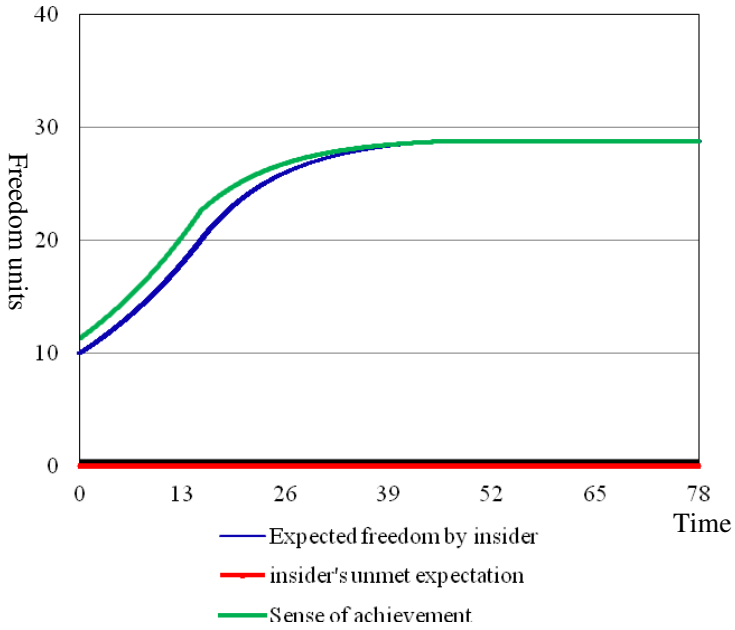


Figure 4. Freedom Growth with Lazy Supervisor

Figure 5 shows the simulation results with Employee A forfeiting Partner status, as represented by the drop in sense of achievement to 10, which is the relative freedom of an insider abiding by that policy. Coincident with the drop is a commensurate rise in unmet expectations. Expectations rise (about 40% in 20 weeks) much faster than they fall, approaching the original policy level at around week 20 under the assumption of an insider with a strong sense of entitlement. Barring any additional loss of freedom, however, expectations do fall gradually as

the insider comes to accept his new situation. Nevertheless, the period of high unmet expectations is one of high risk for the organization, as explained below. The additional drop in the sense of achievement is also explained below.

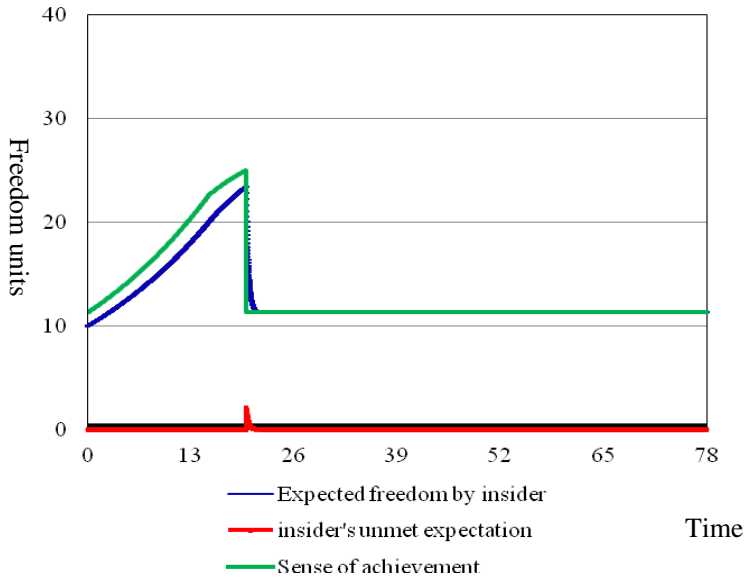


Figure 5. Expectations and Sense of achievement

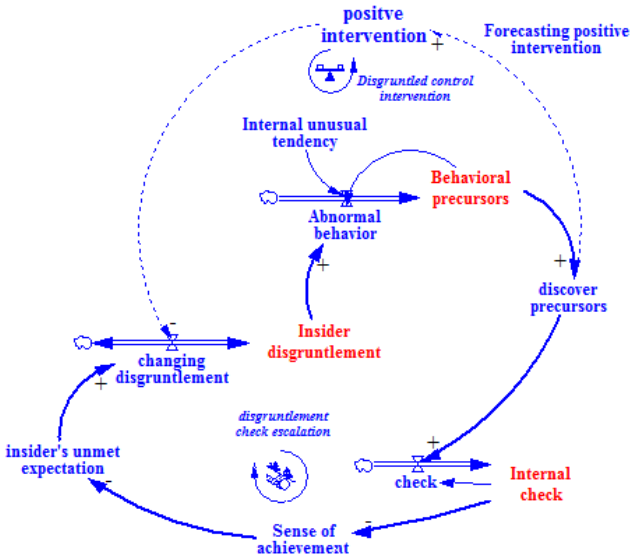


Figure 6. Escalation of Disgruntlement and Internal checks

Figure 6 depicts part of the model: the influence of unmet expectations on the insider's behavior, and the organization's response. Three additional variables are introduced:

(1)Insider disgruntlement: the insider's internal feelings of discontent due to demands or restrictions by the organization that he perceives as unacceptable or unfair.

(2)Behavioral precursors: observable aspects of the insider's offline/social behavior inside or outside the workplace that might be deemed inappropriate or disruptive in some way.

Internal checks: the organization's punitive response to inappropriate behaviors. Internal checks can be technical, such as restricting system privileges or the right to use the organization's equipment at home, or non-technical, such as demotion or formal reprimand. A generic measure of relative severity is used to measure behavioral precursors, damage, and disgruntlement. The reinforcing loop of disgruntlement, checks and escalation in Figure 6 characterizes the escalation of disgruntlement in response to internal checks for inappropriate social behaviors. As the insider's unmet expectations increase, his disgruntlement increases. Insiders exhibit disgruntlement by acting inappropriately offline. Observable inappropriate offline behaviors vary; some insiders take revenge primarily online, exhibiting fewer offline precursors. We assume that the insider's predisposition to disgruntlement indicates his tendency to engage in inappropriate offline behavior before the theft.

Continuing around the loop from disgruntlement to check, the escalation of Figure 6 is affected by the time taken to realize that the insider is responsible. The severity of the actions influences the extent of sanctions, which further limits the sense of achievement. These dynamics explain the second decrease in sense of achievement in Figure 6, after the new supervisor imposes internal checks, further limiting the insider's freedom.

Instead of punitive measures, organizations may take positive actions to address an insider's disgruntlement. Such actions, represented as employee interventions, include referral to an employee assistance program or counseling. The balancing loop from disgruntlement to control intervention in Figure 6 reflects the use of employee intervention to address disgruntlement. The organization's perception of the severity of the behavioral precursors, the observable manifestation of the insider's disgruntlement and the organizational policies determine whether positive interventions and/or internal checks are warranted.

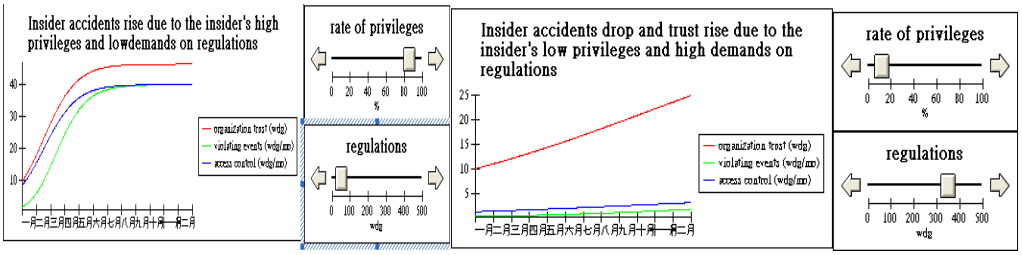


Figure 7. Simulation View

Figure 7 show the increase of insider accidents due to the insider's high privileges (in contrast to the separation of duty) and low demands on regulations. Conversely, if we decrease insider's privileges (conform to the segregation of duty) and demand to comply with rules, the insider accidents reduces and organization trust rises. Another observation shows that, by virtue of building personal behavior profile, any anomaly deviates from the baseline can be detected.

In our option, an insider threat conceptual module should integrate and leverage an array of network and host-based sensors, incorporating a range of cyber observables encompassing a range of classes of physical and cyber actions. The proposed model will use following strategy to mitigate threat：Employee's badge logs, Terminated or stale accounts, Unauthorized access

to peripheral devices, Excessive access to the mission system, Unusual time or frequency using the mission system, Verbal and personal traits.

As management allows the insider's sense of achievement to increase beyond that permit-ted by policy, the insider's expectations also rise. As shown in the figure, expectations and sense of achievement continue to increase at approximately equal rates until about week 40, when freedom reaches a point that even lazy management will not permit — more than twice the freedom allowed by policy. At this point, the insider expects slightly more than is permitted; this situation creates an equilibrium condition where unmet expectations remain fairly constant over time.

The rise of expectations is heavily influenced by the sense of achievement. As illustrated in the reinforcing loop of expectation escalation, with lazy management controls, the sense of achievement grows commensurately with expected freedoms. As more freedom is allowed, more freedom is taken; as more freedom is taken, more is allowed. In the model, it is assumed that even lazy management sets an upper bound on the extent of freedoms allowed to any employees.

In the case given above, Employee A became sufficiently disgruntled to consider the notion of theft. We can detect the following precursor behaviors:

(1)Background：Employee A' s father had also escaped to the United States 10 years ago after forging documents to raise excess loans over NT$100 millions.

(2)Employee A once had the "promotion to partner" opportunity, but because of "the false school record event", the dream of promotion evaporated.

(3)Employee A pretends to be "Employee A's roommate", and asks for the reissue of his identification card and passport.

(4)He set up the nominal "New Emperor Investment Company" and an account related transaction of Asian negotiable securities without authorization.

(5)He asked for an unpaid leave for one year from October 1. The reason was he would prepare to participate in the special attorney examination.

When the precursor behaviors increase, the risk of detecting interior theft increases, and the organization's faith decreases. Furthermore, if the organization's faith is higher, then the need to monitor the technology and the insider control mechanism decrease. The causal loop diagram is shown in Figure 8. A real insider threat case on financial fraud has been analyzed and developed a system dynamic simulation model to facilitate identifying the malicious precursors. The attack threshold can be identified and the understanding the countermeasures of insider threats. Figure 8 models the insider threat case and can be used as a training and education tool for the development of insider threat diagnostic, as well as the improvement of insider threat awareness and mitigation.

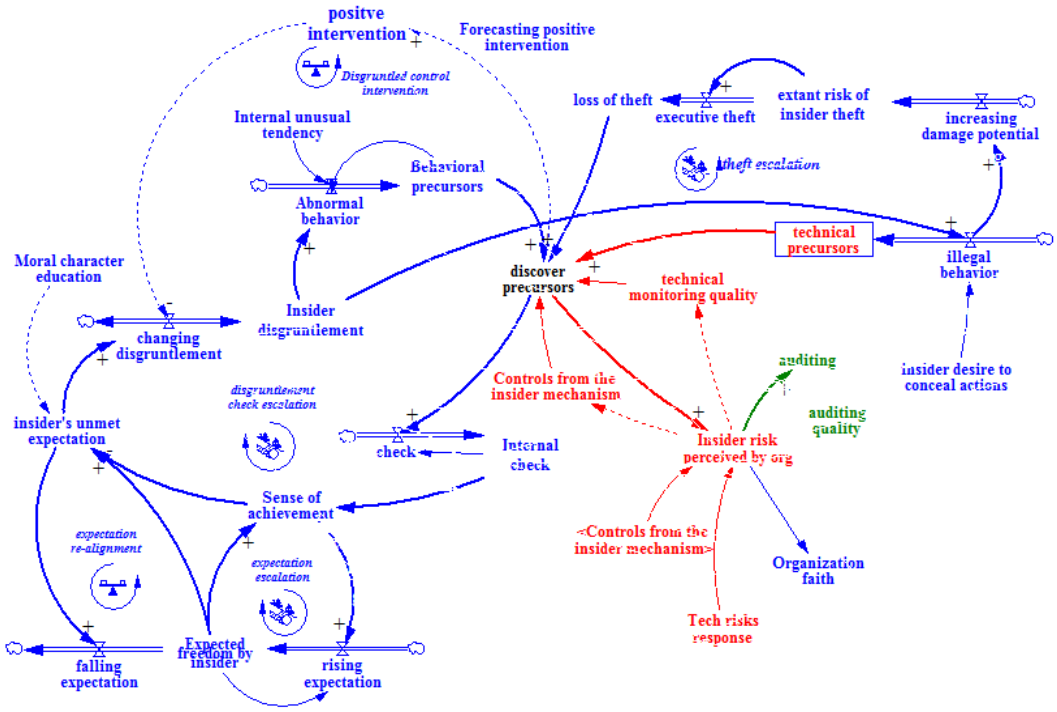


Figure 8. Causal loop of the incident of the well-known enterprise

According to the analysis result, for instance, Employee A requested an unpaid leave suddenly; we are able to detect the exceptional action early through the behavior and to flag it for further analysis. In addition, combining the insider monitoring and the risk control mechanism into the mold process may also reduce the risk and increase the probability of detecting insider threats from personnel. Consequently, we propose two important views for the decision maker:

(1) Executing the insider control and liability insurance mechanism resembles internal auditing, distributed risks, and risk control mechanisms. That will lower the risk of internal theft detection and employee confidence to the lowest possible levels. Furthermore, a correlation technique can detect the malicious motive and behavior at the outset, and then, depending on the access path, enable the early detection of illegal activity and suppress the illegitimate access immediately.

(2) To establish corresponding relationships between the logical organization and the solid structure with correct behavior, constructs files in the database (for example, the establishment of a vulnerable database) to enable us to detect and investigate the exceptional/ illegal activity rapidly and certainly and then to take actions in the early stages to prevent the illegal behaviors.

5. Conclusion

Further calibration and validation of the model is still necessary before it can be released for educational or training use. Extensive user interface testing will be required to develop an intuitive interface and accompanying training materials before it can be used in an actual training class.

Today's network protected systems usually only defend against external attacks but are unable to detect insider attack behaviors effectively. Therefore, this study applies the system dynamic

method to analyze the deviant behavior and develop the insider threat detection embryo model. In the future, we expect to achieve the following goals efficiently and effectively:

(1)Monitoring the user behavior of operating information systems and automatically establishing a normal user behaviors profile.

(2)To develop the compatible technology to distinguish indications of the triggers of possible deviant behavior.

(3)To detect possible deviant behavior immediately and reduce the detection time of the deviant internal behavior.

(4)To increase the working efficiency of the system monitoring and administration by reducing a large amount of the unusual record that must be scrutinized.

Because industries and government organizations do not open and share their current information security conditions, data collection is the most critical work in the modeling process of the insider threat detection model. We can only dependent on an appropriate open policy, cooperating with research and development in information technology, so as to minimize the risk of insider threat. Insider threat is a complicated security issue. There are few good tools and techniques that can be used to calculate the threat. We do believe that we have made a significant advance by proposing a usable and generic threat assessment model and demonstrating its applications to the classic insider threat case. We suppose that system dynamics modeling is more generic and may have appeal beyond just insider threat analysis.

There is no single silver bullet solution to this problem. Further, the main factors of the model can help organizations build information security into the early stages of the production life cycle to minimize risk through the rapid development of software.

When the information security requirements of organizations are considered at all during the system life cycle, they tend to be general lists of security features. In fact, these are not only security requirements but rather implementation mechanisms that are intended to satisfy unstated requirements. The need for security requirements that are specific to the information system and that provide for protection of essential services and assets is often neglected. We believe that a systematic approach to security requirement engineering will help avoid the problem of generic lists of features and take into account the insider perspective.

The study of insider threat is a challenging research area. We believe that the application area, the approach, and the model described herein will be of interest to researchers in the area of insider threats.

REFERENCES

[1] CSO magazine in cooperation with the U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte. 2010 CyberSecurity Watch Survey – Survey Results, 2010.

[2] M.R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. US Secret Service and CERT Coordination Center, 2004.

[3] W.D. Maughan, Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Require Strategic Investment and Immediate Action. House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. iCAST technical report. Taiwan, pp. 18-19, 2007.

[4] R. Moore, "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing, 2005.

[5] D.M. Cappelli, A.G. Desai, A.P. Moore, T.J. Shimeall, E.A. Weaver, B.J. Willke et al, Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage. Joint CERT Coordination Center/SEI and CyLab at Carnegie Mellon University Report, Pittsburgh, PA, pp. 1-34, 2006.

[6] R.H. Anderson, Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. RAND Corporation, Santa Monica, CA, pp. 1-43, 1999.

[7] E.E. Schultz, A framework for understanding and predicting insider attacks, Computers and Security 21, pp. 526–531, 2002.

[8] S. Symonenko, L. Liddy, O. Yilmazel, R. Del Zoppo, E. Brown, M. Downey. Semantic analysis for monitoring insider threats. IEEE Intl. Conf. on Intelligence and Security Info, 2004.

[9] A. Liu and C. Martin, A Comparison of System Call Feature Representations for Insider Threat Detection. Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, pp. 340-347, 2005.

[10] R. Chinchani, A. Iyer, H.Q. Ngo, S. Upadhyaya, Towards a Theory of Insider Threat Assessment, Proceedings of the 2005 International Conference on Dependable Systems and Networks, Yokohama, Japan, pp. 108–117, 2005.

[11] J.S. Park and J. Giordano, Role-Based Profile Analysis for Scalable and Accurate Insider-Anomaly Detection. Proceedings of the 25th IEEE International Performance Computing and Communications Conference, Workshop on Information Assurance, Phoenix, AZ, pp. 463-469, 2006.

[12] M. Maybury, Detecting malicious insiders in military networks. MILCOM-06, Washington, DC, pp. 1-7, 2006.

[13] Jonathan W. Butts, Formal Mitigation Strategies for the Insider Threat: A Security Model and Risk Analysis Framework. On-line document, https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q_act_downloadpaper/q_obj_9390d5ea-5e71-4abb-b3e6-c03c79975762/display.aspx, 2006.

[14] D. Ha, S. Upadhyaya, H. Ngo, S. Pramanik, R. Chinchani, S. Mathew, Insider threat analysis using information-centric modeling, in IFIP International Federation for Information Processing, Volume 242, Advances in Digital Forensics III, pp. 55-73, 2007.

[15] G. Ali, N.A. Shaikh, Z.A. Shaikh, Towards An Automated Multiagent System to Monitor User Activities Against Insider Threat. Proceedings of the International Symposium on Biometrics and Security Technologies, IEEE-ISBAST 2008, Islamabad, Pakistan, pp. 1-5, 2008.

[16] M. McCormick, Data Theft: A Prototypical Insider Threat. In Advances in Information Security, 2008

[17] M. Chagarlamudi, B. Panda, Y. Hu, Insider Threat in Database Systems: Preventing Malicious Users' Activities in Databases. In: Proceedings of the 2009 SixthInternational Conference on Information Technology: New Generation, Las Vegas, pp. 1616 – 1620, 2009.

[18] G. Jabbour and D.A. Menasce, The Insider hreat Security Architecture: A Framework for an Integrated, Inseparable, and Uninterrupted Self-Protection Mechanism. Computational Science and Engineering, CSE '09. International Conference on, pp. 1616 – 1620, 2009.

[19] S. Nellikar, Insider threat simulation and performance analysis of insider detection algorithms with role based models. MS thesis. University of Illinois at Urbana-Champaign, Urbana, IL, 2010.

[20] R. H. Anderson, T. Bozek, T. Longstaff, W. Meitzler, M. Skroch, K.V. Wyk, Research on Mitigating the Insider Threat to Information Systems-#2. Proceedings of a Workshop Held, RAND Corporation, Santa Monica, 1-35, 2000.

[21] Matt Bishop , Carrie Gates, Defining the insider threat, Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, May 12-14, 2008.

[22] J.F. Van Niekerk, R. Von Solms, Information security culture: A management perspective, Computers & Security, Volume 29, Issue 4, pp. 476-486, 2010.

[23] M.M. Keeney, E.F. Kowalski, D.M. Cappelli, A.P. Moore, T.J. Shimeall, S.N. Rogers et al, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Joint SEI and U.S. Secret Service Report, Pittsburgh, PA, 1-45, 2005.

[24] D.M. Cappelli, A.G. Desai, A.P. Moore, T. Shimeall, E.A. Weaver, B.J. Willke, Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage. In Proceedings of the 24th Conference of the System Dynamics Society, 2006.

[25] Stephen R Band, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, Randall F. Trzeciak, Comparing Insider IT sabotage and espionage: A Model based Analysis., CMU/SEI-2006-TR-026, 2006.

[26] D.M. Cappelli, A.P. Moore, T.J. Shimeall, R.F. Trzeciak, Common Sense Guide to Prevention and Detection of Insider Threats. Carnegie Mellon University Report, Pittsburgh, PA, Second Edition, 1-43, 2006.

[27] F.L. Greitzer, A.P. Moore, D.M. Cappelli, D.H. Andrews, L. Carroll, T.D. Hull, Combating the Insider Cyber Threat. IEEE Security & Privacy 6(1):61-64, 2008.

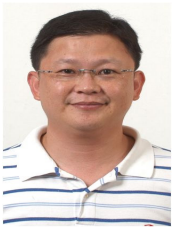
[28] A. P. Moore, D. M. Cappelli, R. F. Trzeciak, The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures. Tech Rep CMU/SEI-2008-TR-009, 2008.

[29] Jay W. Forrester, Industrial Dynamics. Pegasus Communications. ISBN 1883823366, 1961.

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

Authors

Sang-chin Yang received his Bachelor of Science degree in civil engineering from CCIT in 1988. He earned his Master of Science degree in systems engineering in 1994 and Doctor of Philosophy degree in industrial and systems engineering in 1999, both from Virginia Polytechnic Institute and State University. His research interests focus on information assurance and security, reliability theory, maintenance policies, supportability engineering, systems engineering, technology management, and decision theory.



Yi-Lu Wang received the B.S. and the M.S. degree in Electrical and Electronic Engineering, both from Chung Cheng Institute of Technology (CCIT), National Defense University, Taiwan, R.O.C., in 1997 and 2004, respectively. He is currently pursuing the Ph.D. degree in the area of information security at CCIT. His research interests are focused on information security and decision theory.