Advanced Computing: An International Journal (ACIJ), Vol.2, No.2, March 2011

Insider Threat Analysis of Case Based System Dynamics

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

One of the most dangerous security threats today is insider threat, and it is such a much more complex issue. But till now, there is no equivalent to a vulnerability scanner for insider threat. We survey and discuss the history of research on insider threat analysis to know system dynamics is the best method to mitigate insider threat from people, process, and technology. In the paper, we present a famous case of insider threats in Taiwan using system dynamics to analyze the tailored model. We may reduce the risk and increase the probability of detecting insider threats from personnel of simulation model. The study concludes with suggestions for future research and implications for system dynamics who are interested in insider threat issue.

KEYWORDS

Case Based, System Dynamics, Insider Threat

1. Introduction

Network and information technologies occupy a pivotal position in critical infrastructures, but they are changing due to rapid innovation constantly. The issue of information security is increasingly important for homeland security. However, the greatest threat to information systems, such as important national defense and critical infrastructure, is often an insider threat. The 2010 CyberSecurity Watch Survey [1] posits that multiple attacks can occur within larger organizations, and insiders remain the most costly threat. Insider incidents are more costly than external breaches, according to 67% of respondents. CERT has been working with government and industry leaders to develop recommendations for new solutions to this problem using commercial and open source tools, and has invited organizations to share their insights, according to Dawn Cappelli. However, 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. Unfriendly insiders can be the main threats to an organization. Given the limited ability of existing systems to counter abnormal insider behaviour s, 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 behaviour s. 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. The hearing named "CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: THE THREAT IS REAL" examined a growing public policy concern, the threat of hostile attack on U.S. critical information infrastructure and the adequacy of the Federal Government's response to this threat. One of the categories of individuals is probably

DOI : 10.5121/acij.2011.2201

the most common, and that is the disgruntled insider is a principal source of computer crimes. Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of victim systems often allows them to gain unrestricted access to cause damage to the system or to steal system data. So there is an incredibly broad array of threats in the cyber area that we have to deal with, and one of the difficulties in this area that distinguishes it qualitatively from the physical world is that when you first notice that you have an intrusion, you do not know what you are dealing with. You do not know if it is a disgruntled insider, if it is an organized crime group, if it is a terrorist, a foreign intelligence agency, or a nation state planting the seeds for future destructive attacks. There are many cases in the public domain involving disgruntled insiders. For example, Shakuntla Devi Singla used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1,800 hours to recover and reentered the lost data. Ms. Singla was convicted and sentenced to five months in prison, five months home detention, and ordered to pay $35,000 in restitution. In another case, a former Forbes employee named George Parente hacked got into Forbes systems using another employee's password and login identification and crashed over half of Forbes' computer network servers and erased all of the data on each of the crashed services. The data could not be restored. The losses to Forbes were reportedly over $100,000 [2]. The document represents the culmination of a 2-year effort by the Information Infrastructure Group (IIG) of the President's National Security Telecommunications Advisory Committee (NSTAC) to study the information-based risks to the United States transportation information infrastructure. Transportation Information Infrastructure Risk Assessment Report of NSTAC also discussed the potential for insider threats to transportation companies was increasing in 1999. The insider threat has historically been disgruntled employees exploiting their knowledge of a company to gain unauthorized access into sensitive corporate systems. The motive is often revenge or blackmail. However, industry representatives noted that their definition of an insider has expanded to include employees of a business partner of the company who is not under their immediate control, such as a subcontractor, supplier, or customer. As globalization, consolidation, corporate downsizing, and intermodalism increase, transportation companies will increasingly turn to outsourcing and strategic alliances to meet their business needs. This change in how they conduct business is likely to expose them to additional insider threats. [3].

Insider Threat Study [4]: Insiders can be stopped, but stopping them is a complex problem. Insider theft can only be prevented through a layered defense strategy consisting of policies, procedures, and technical controls. Therefore, management must pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment. 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 [5] 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 [6]. 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 [7] 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. Section 5 concludes the paper with an overview of our future research directions.

2. Related work

We present the summary of the research in insider threat analysis from 1999 to 2010. We have to classify people, process and technology in these articles and most of them focus on technology.

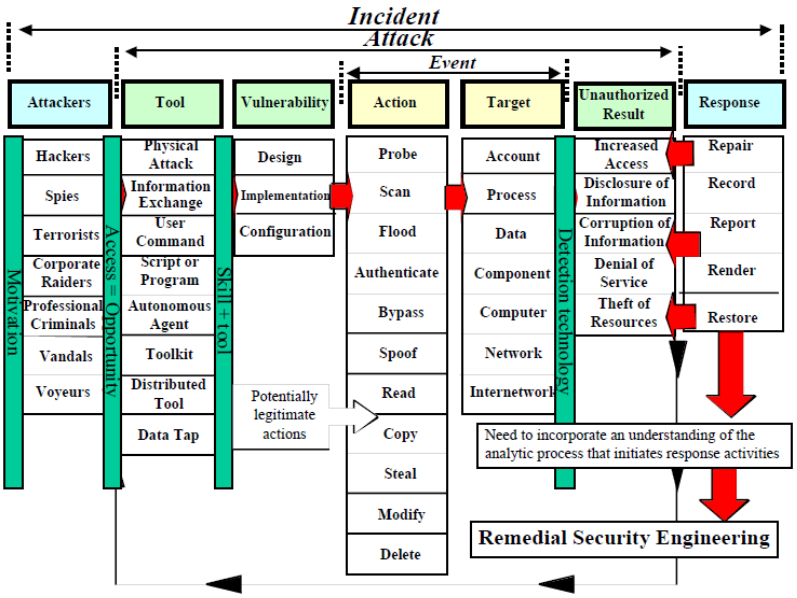

Figure 1. Characterizing an information system security incident [8]

Anderson (1999) proposes the results of a Three-Day Workshop about insider threat issue. The policies and procedures are needed to form an environment for mitigating the insider threat. And the insider threat is not unique unto itself; it is part of overall information system security. Workshop discussions and breakout groups used the addressing threats and vulnerabilities, prevention, detection, and response in describing possible research initiatives. The experts in the workshop modified a JTFCND (Joint Task Force – Computer Network Defense) graph to provide an overview of the distinctions among an incident, an attack, and a specific event as Figure 1. Figure 1 also indicates the roles of an attacker's motivation combined with access, plus use of skills and tools, and shows the role of detection technology when an event has occurred [8]. Schultz (2002) presents a framework for predicting and detecting insider attacks. It may indeed be possible to predict and detect insider attacks with multiple indicators and a mathematical representation of each indicator's contribution. The framework present promising in that it synthesizes and builds upon critical models and findings concerning insider attacks, but unproven. They indicate 6 different potential indicators of internal attacks exist and that no single indicator can normally provide conclusive indication of an insider attack. These potential indicators include: deliberate markers, meaningful errors, preparatory behaviour, correlated usage patterns, verbal behaviour, personality traits as Figure 2 [9]. Symonenko et al prove (2004)

Natural Language Processing (NLP) system to integrate the results of social network analysis, role-based access monitoring, and semantic analysis of insiders' communications. The analysts' tasks were modelled on scenarios developed by the Center for Non-Proliferation Studies (CNS) 7 experts for use in ARDA's AQUAINT (Advanced Question and Answering for Intelligence) Program, and the authors also make use of the scenario based questions generated at the 2003 ARDA-NRRC workshop on Scenario-Based Question-Answering. The majority of the prior research focuses on a particular genre, and it also further investigates benefits and issues related to an ontology-driven approach to identifying important topical structures in large and stylistically diverse datasets [10].

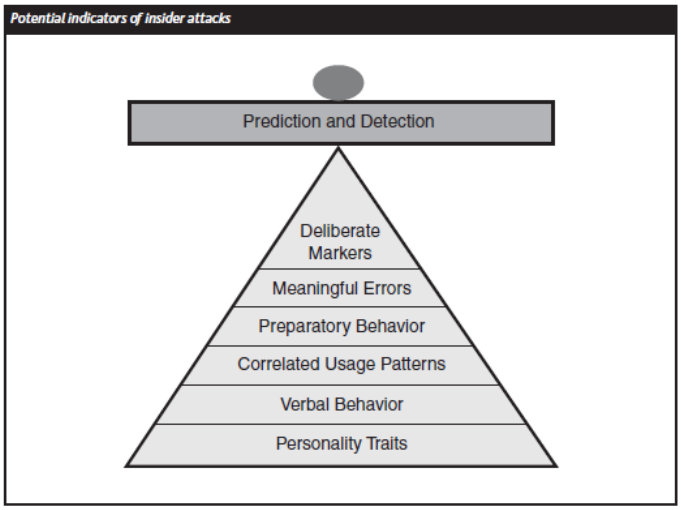

Figure 2. Potential indicators of insider attacks [9]

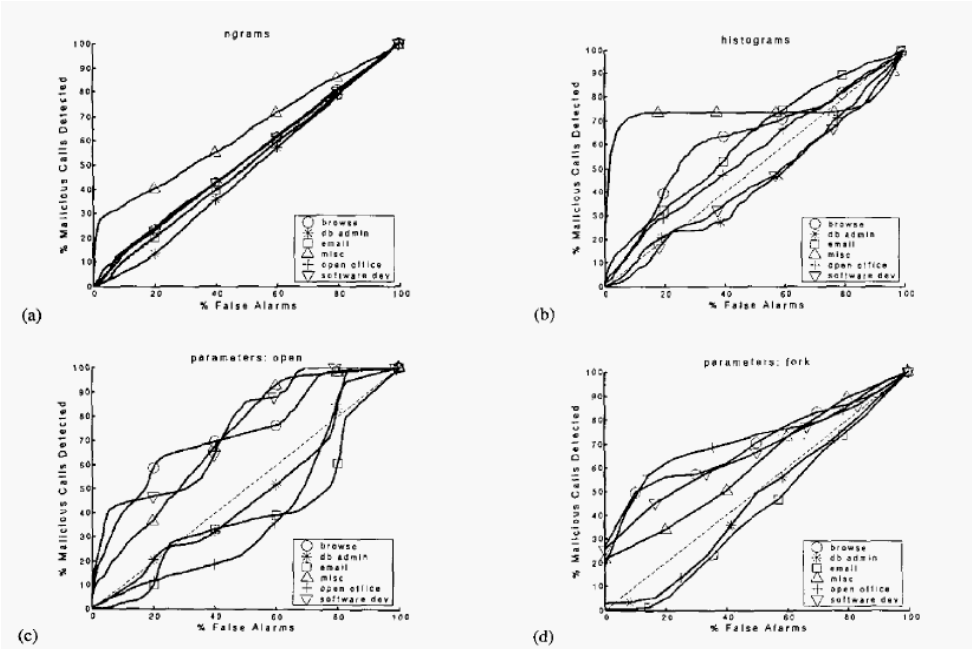

Figure 3. ROC Curves for detection performance [11]

Liu and Martin (2005) analyze the sensitivity to malicious insider activity of different feature representations using a k nearest neighbor outlier detection algorithm, and three different types of feature representations are compared in the form of Unix system call information. They suggest that future work should focus on parameter-based features to find leverage for detecting unusual behavior as malicious. Figure 3 (a, b, c, and d) shows the performance on each of the datasets for each feature representation [11]. Maybury (2006) reported results from a challenge workshop to summarize and characterize the automatic detection of malicious insiders within modern information systems. He demonstrated how an integration of multiple approaches promises early and effective warning and detection for a range of insider threats. Key lessons learned from the malicious insiders (MI) research include the need to understand the context of the user's actions, the need to establish models of normal behavior, the need to reduce the time to detect malicious behavior, the value of non cyber-observables, and the importance of real-world data collections to evaluate potential solutions [12]. Figure 4 is one of the challenge workshop which illustrates the heterogeneous nature of the collection consisting of over 11 million records.

Figure 4. Insider threat challenge workshop : event and observable taxonomy [12]

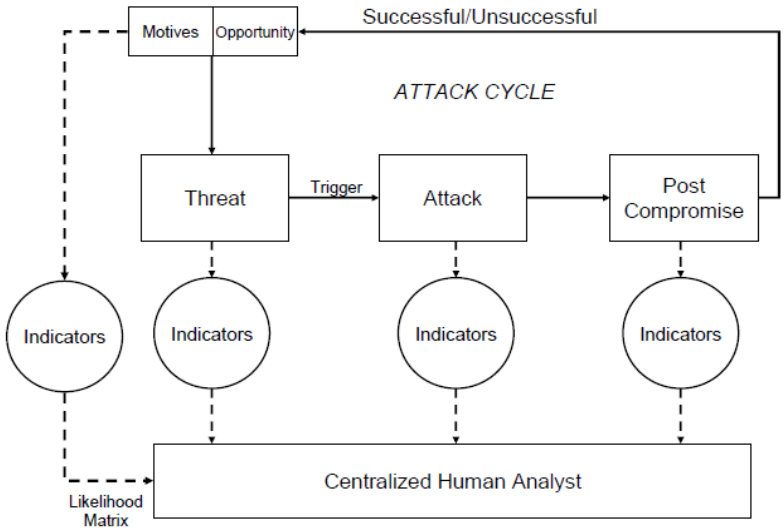

Figure 5. Multidisciplinary framework for mitigating the insider threat. [13]

Butts (2006) 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]. The goal of the Multidisciplinary Approach to Mitigating the Insider Threat (MAMIT) is identification of suspicious individuals within an organization that display a credible amount of threat so follow-up action can be taken. Figure 5 illustrates the proposed cohesive process for countering the malicious insider. The Multidisciplinary Approach to Mitigating the Insider Threat (MAMIT) is the framework designed to perform risk analysis for the insider threat. Ha et al. (2007) describe a novel CAG-based tool called ICMAP (Information-Centric Modeler and Auditor Program) and demonstrate the feasibility of applying capability acquisition graphs to insider threat analysis [14]. The ICMAP shown as Figure 6 presented in this paper is very effective at modelling insider threats, analyzing vulnerabilities and evaluating sensor deployment locations.

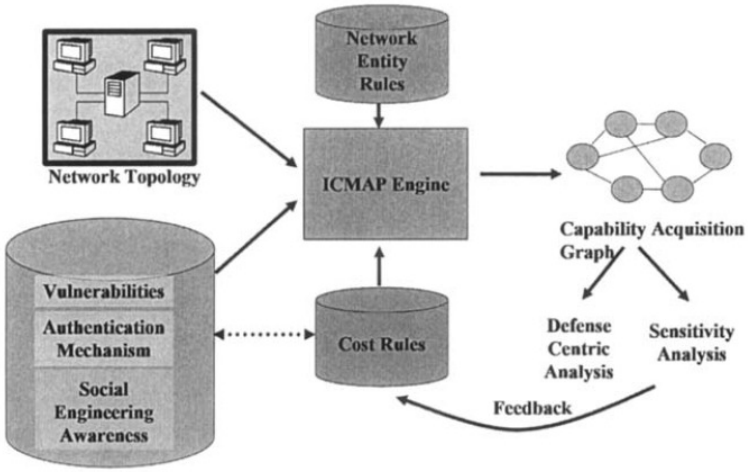

Figure 6. ICMAP framework [14]

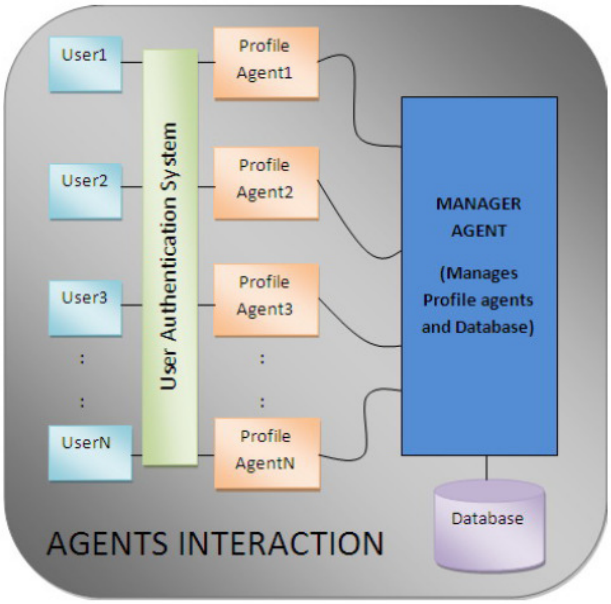

Figure 7. Authentication system and agents interaction [15]

Ali et al. (2008) present an Agent-based User-Profiling model shown as Figure 7 which builds and maintains the profile of all the insiders. The profile is dynamic in nature that is being updated continuously while monitoring the behaviour of an insider. The presented model also monitors the behavior of the authorized users in an organization to avoid risk [15]. McCormick (2008) assesses the threat of confidential data leakage, focusing on its most virulent form insider data theft attacks. He describes a comprehensive EDLP strategy which can mitigate inadvertent leakage as well as intentional data theft and reduce the risk of a large or embarrassing "data spill" in most modern automated enterprises. Figure 8 shows the three stages of data leak or theft, along with an example involving a malicious Oracle DBA, plus some common security controls applied at each stage of the leak [16].

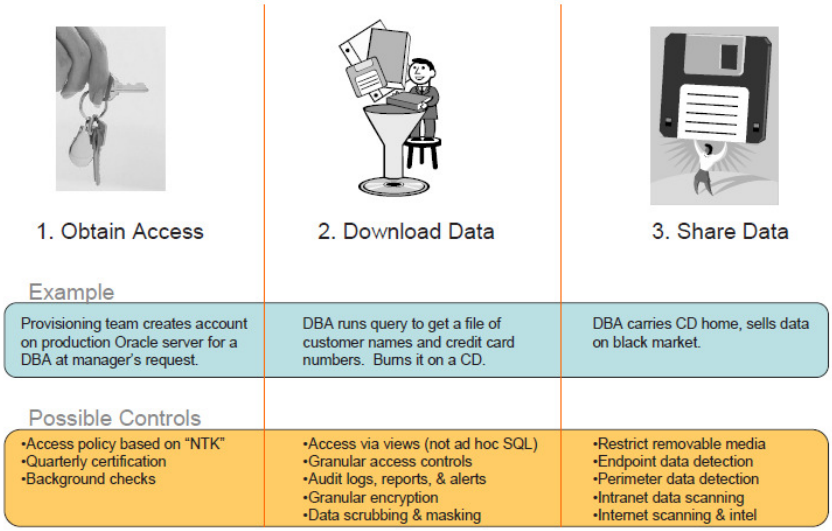

Figure 8. Stages of data theft [16]

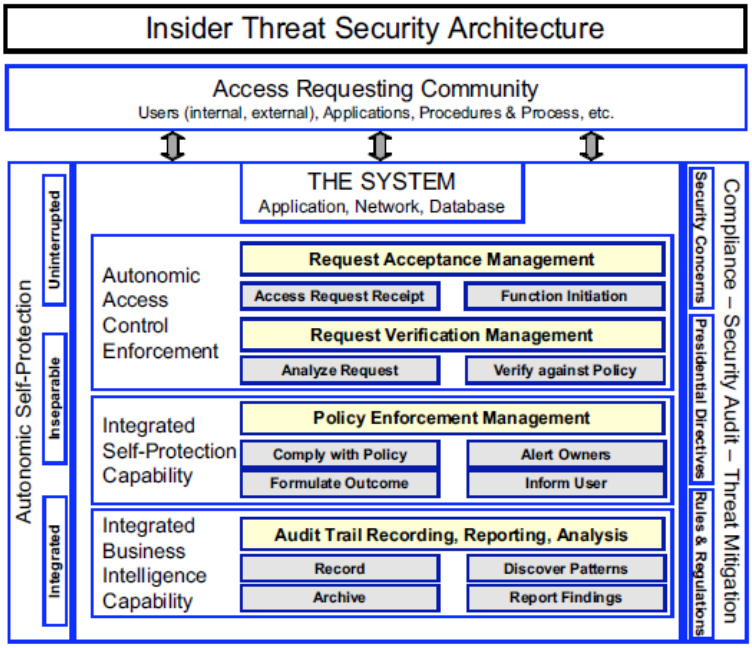

Figure 9. The insider threat security architecture framework [17]

Jabbour and Menasce (2009) 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. The ITSA framework, shown as figure 9, is built on the foundational notion that any protection mechanism must be totally integrated into, and inseparable from the system that is being protected in such a way that the protection process cannot be interrupted [17]. Nellikar (2010) focuses on the advantages of using role based mechanisms for insider threat detection. Nellikar presents the simulator is built on the Scalable Simulation Framework (SSF), and JANUS is an extension of the Boeing simulator which uses behavior files to model an insider/normal user and generates the access information using Markov chains. The presented simulator is compatible with the JANUS simulator. A block diagram of the system is given in Figure 10 [18].

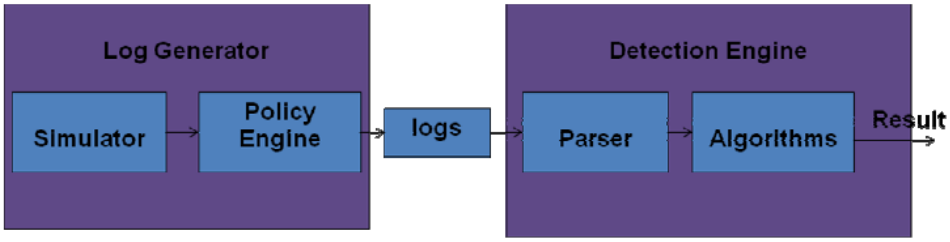

Figure 10. Simulation system of scalable simulation framework [18]

Process-classified articles are described next 3 papers. Anderson's paper (2000) "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems" summarizes the findings and recommendations resulting from 2-day workshop which addresses 4 categories for insider threat [19]. Figure 11 provides a graphic depiction of the model framework.

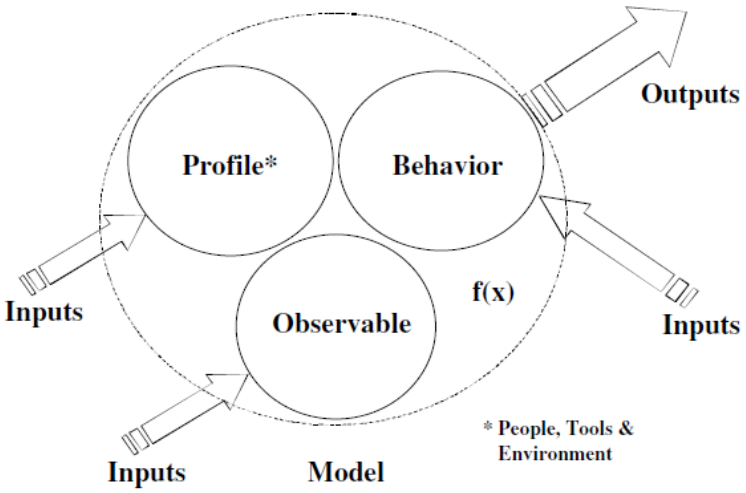

Figure 11. A high level diagram for the model structure [19]

Bishop and Gates' article (2008) "Defining the Insider Threat" presented an initial approach to defining insiders based on their access attributes, and hence the insider threat problem. Ordering protection domains based on their value to group them by their value of their protection domains, the paper can provide a continuum of insiders [20]. Niekerk and Solms (2010) present

a conceptual model to facilitate conceptual thinking and argumentation in the culture of information security. The conceptual model can present showed that the overall effect that an information security culture would have on the organization's information security efforts would depend on the relative desirability, or strength, of each underlying level in such a culture. [21].

However, we believe that all these studies have neglected a crucial element: people. Keeney (2005), Cappelli (2006-2007), Band (2006), Greitzer (2008), and Moore et al. (2008) have all used system dynamics to prevent insider threat [22-27]. But we know that the method not only embraces technology, but also includes process and people. In this paper, we analyze these articles of insider threat, and choose the case based system dynamics inclusive of people, process and technology been the methodology of prevention insider threat.

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 behaviour 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 behaviour pattern and take appropriate measures.

Table 1. 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 12. We also know that lazy management unintentionally encouraged the escalation of expectations, as seen in the simulation results in Figure 13. 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.

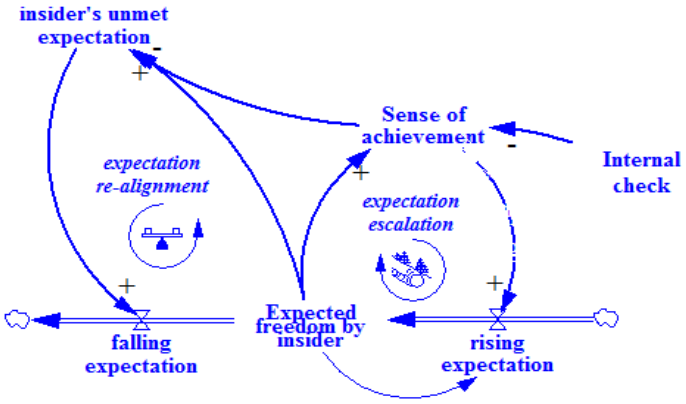

Figure 12. Expected freedom by insider

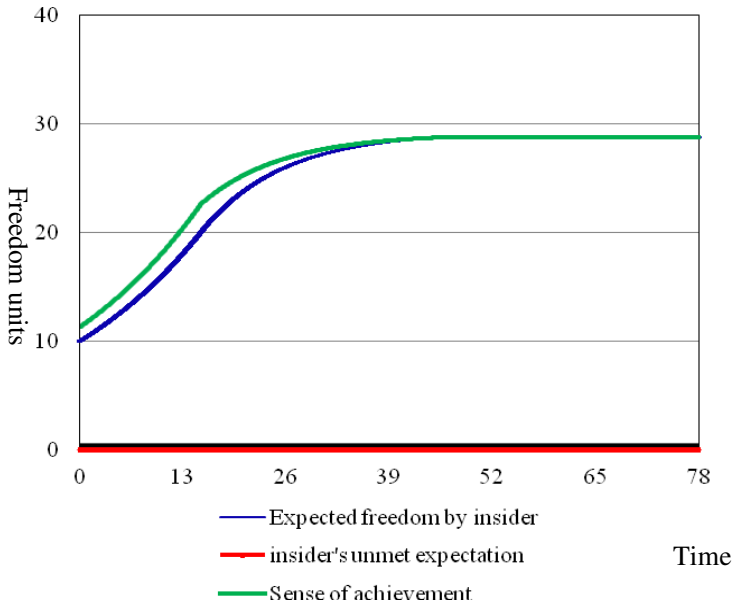

Figure 13. Freedom growth with lazy supervisor

Figure 14 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.

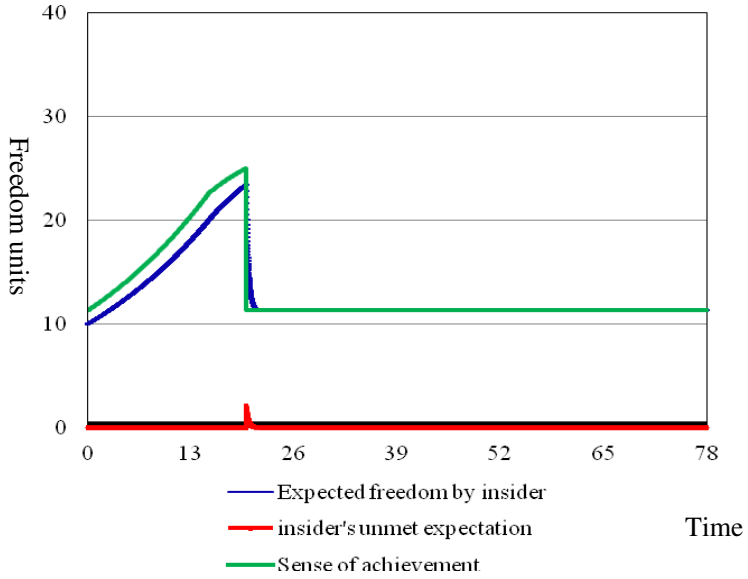

Figure 14. Expectations and sense of achievement

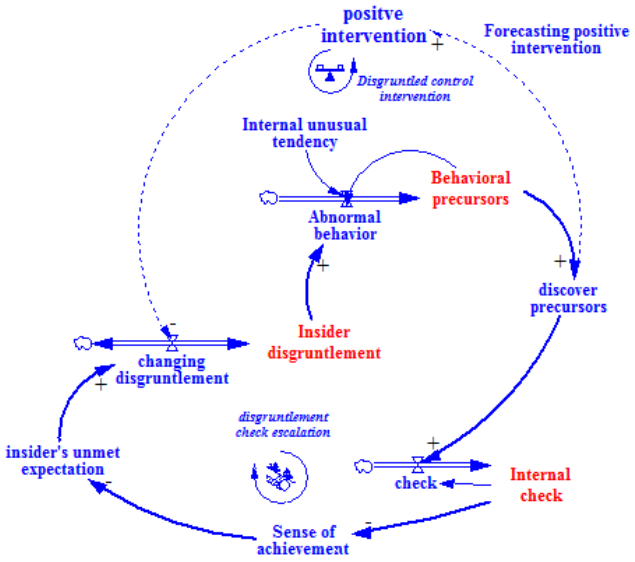

Figure 15. Escalation of disgruntlement and internal checks

Figure 15 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 15 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 15 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 15, 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 15 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.

As noted above, an organization's full awareness of the access paths available to an insider is critical to its ability to disable those access paths when needed.

As management allows the insider's sense of achievement to increase beyond that permit-ted by policy, the insider's expectations also rise. 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 2003. 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 16.

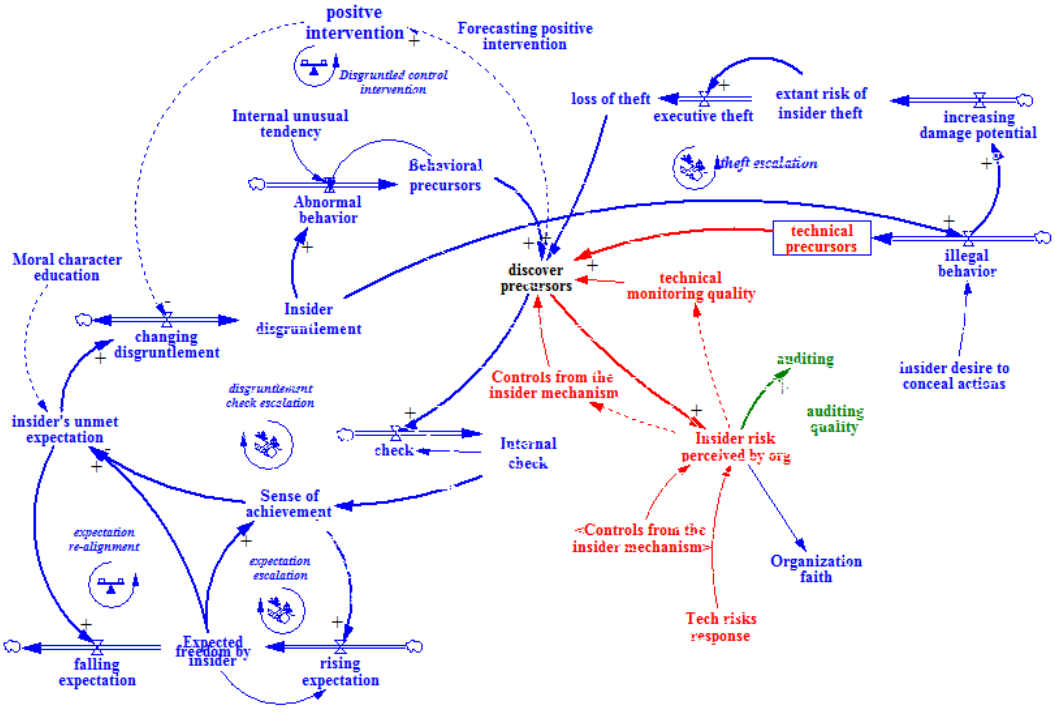

Figure 16. Causal loop of the incident of the well-known enterprise

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

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. The study of insider threat is a challenging research area. We do believe that 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] Senate Hearing 106-858 - Critical Information Infrastructure Protection: The Threat is Real, 1999.

[3] Transportation Information Infrastructure Risk Assessments Report of the President's National Security Telecommunications Advisory Committee, 1999.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[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] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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.