Internal Control of Secure Information and Communication Practices through Detection of User Behavioral Patterns

Suchinthi A. Fernando and Takashi Yukawa

***Abstract*—This paper proposes a solution to the human-related information security problem of improper sharing of information by insiders with outsiders or unauthorized insiders. As opposed to most currently available solutions, this system does not rely solely on technological security measures, but proposes a mixture of social and technological solutions. The proposed system hopes to monitor users' security behavioral patterns and create behavioral profiles and thus identify users who might pose potential threats to the organization's information security. The system will further provide security education and training to identified users. The authors are currently developing the proposed system.**

***Index Terms*—human behavior, information security, profiling, social, technological**

I. Introduction

THE focus of information security has shifted from being "technology-oriented" to "management-oriented" [1] during the past decade. In order to succeed in business, it is mandatory to ensure that access to information is strictly limited to the personnel who need to know it in order to perform their assigned tasks [2]. Yet, most identified information security breaches occur because of human errors [3], resulting from lack of proper knowledge and training, ignorance, and failure to follow procedures. People's beliefs and expectations may lead to mistakes and misjudgments of risks [4]. Thus, being the weakest link in the chain of security, people may unintentionally reveal confidential information to others. Schneier [5] explains how the perception of security diverges from its reality and how people feel secure as long as there is no visible threat. This human weakness is exploited in most present-day attacks, which require a human element, to succeed [6]. These attacks may come in the forms of social engineering, spear phishing, or collusion from an insider, where people are tricked into revealing confidential information.

Effective information security uses physical, technical, and operational controls, where operational controls concern the conduct of employees with regard to information security [7]. Even though information systems security auditing ensures that an organization's security policies, procedures, and regulations are effective, auditing is not performed on the employees, instead their adherence to these audited policies is automatically assumed [7]. Thus, it can be seen that despite the overall understanding that the human factor should be taken into consideration in information security management (ISM), most security solutions available today still rely on purely technical measures to enforce information security. Yet, people may easily bypass technological controls and restrictions such as access control by revealing their authentication information to others. Vroon and von Solms [7] state that: "Human behavior is not performed according to a set of written rules, but according to the personality of the individual… However, this behavior can be categorized."

This paper addresses the problem of improper sharing of information and proposes a mix of technological and social solutions to achieve internal control of information and communication within an organization. This solution entails the monitoring of the levels of observance of secure practices by its employees in order to create employee behavioral profiles by categorizing employees' security behavior, and thus identifying employees whose actions could potentially lead to ISM problems and therefore require special education and training in ISM.

II. Threat Detection and Sustainable Security

Studies concerning intrusion detection systems prevail in the field of information security. Yet, 60%-70% of attacks originate from the inside with the involvement of "trusted" folks and are more expensive than external attacks [8]. The inclusion of users with non-malicious intent raises the percentage of insiders wittingly or unwittingly involved in an attack to at least 80% [9]. An intrusion of an information system is defined as "an activity that violates the security policy of the system", and intrusion detection is the process to identify intrusions based on the belief that the intruder's behavior will be noticeably different from that of a legitimate user and that many unauthorized actions will be detectable [10]. On the contrary, insider threat is defined as "trusted users with legitimate access abusing system privileges" [11] or as "intentionally disruptive, unethical, or illegal behavior enacted by individuals possessing substantial internal access to an organization's information assets" [12]. Insider attacks are indistinguishable or difficult to distinguish from normal actions as inside attackers have

Manuscript received March 15, 2013; revised April 03, 2013.

S. A. Fernando is a doctoral student in the Department of Information Science and Control Engineering, Nagaoka University of Technology, Nagaoka, Niigata 940-2188 Japan (phone: (+81)90-30992350; e-mail: s095191@stn.nagaokaut.ac.jp).

T. Yukawa is with the Department of Management and Information Systems Science, Nagaoka University of Technology, Nagaoka, Niigata 940-2188 Japan (e-mail: yukawa@vos.nagaokaut.ac.jp).

authorization to access and use the system and these actions are less likely to differ from the norm [11]. Database administration, word processing, web browsing, command-prompt interaction, etc. are considered as normal activities, while exploitation, extraction, manipulation, reconnaissance, access, and entrenchment are categorized as malicious insider activities [11]. Insider attacks are difficult to detect until after damage has been done, and attempts to solve these may exacerbate problems or introduce new problems. Yet, since most insider attacks are planned, there is a window of opportunity during which people can intervene before the attack has occurred and prevent attack or limit damage [12].

Even though most technical security measures may be somewhat sufficient to keep the outside attacks at bay, technical measures alone are clearly insufficient to ward off insider attacks. Sabett [13] states that any security system should be designed by accepting that the “bad guys” are already inside your system, and instead of having a hardened shell and a soft core, the most sensitive parts of the system or network should be hardened. A holistic approach blending people, process, and technology by focusing on behaviors and activities appearing to be risky using a combination of risk management, functional analysis of insider behaviors, and risk mitigation (evaluation and selection of control measures) is recommended [12]. Observable behaviors include cyber activities, which only provide limited insight into intent and character, but are easier to collect, process, and correlate automatically, as well as personal conduct, which is observed through background checks [12]. Employees may be divided based on their current level of awareness of the information security objectives [14]. Conducting a “walkabout” after normal working hours to look for key indicators such as whether the offices, desks, and cabinets are locked, workstations, information, and recording media are secured, etc. helps to determine these levels. Personnel may also be categorized according to job category, job function, their knowledge about information processing, and technology, system, or application used [14]. Accidents will not normally happen if security measures stay above a certain threshold and the risk is kept below the “accident zone” [15]. Perceived risk gradually declines when accidents do not occur as a consequence of improved security, leading to a decline in the compliance with security measures until system becomes vulnerable again. Thus, risk perception renewals through properly scheduled interventions such as security training and awareness programs are needed in order to sustain an appropriate level of risk perception [15]. Foley [16] lists the following components as requirements for a proactive and sustainable security program: preventive (credentialing the employees, clients, and vendors, and restricting access through authorization of identity, time, and place), detective (auditing, monitoring, and referrals to validate allegation and determine if the use was fraudulent or legitimate), corrective (additional monitoring or auditing, update credentials, access restriction, or access removal), and feedback (dynamic, reactive, and planned feedback and creating and implementing solutions).

The system proposed in this paper incorporates these suggestions by blending social and technological solutions to monitor cyber and non-cyber activities of users, detect patterns among these behaviors, and use this information together with background information and job details to create security behavioral profiles of users, in order to identify users who might potentially be problematic. In order to better understand the security profiling techniques to be adapted for the proposed system, the next section explores different profiling techniques including those currently used in other areas of security.

III. Security Profiling

Lacey [1] states that the Myers & Briggs Type Indicator (MBTI) instrument could be used to categorize user psychological types and would therefore enable profiling to be applied to information security.

A. Myers & Briggs Type Indicator (MBTI)

MBTI is based on Carl Jung’s Theory of Psychological Types, which states that much seemingly random variation in behavior is actually quite orderly and consistent, being due to basic differences in the way individuals prefer to use their perception and judgment [17]. MBTI uses Jung’s ideas to identify basic preferences of each of the four dichotomies specified in Jung’s theory and to identify and describe the sixteen distinctive personality types resulting from the interactions among the preferences. Perception is defined as “all the ways of becoming aware of things, people, happenings, or ideas”, while judgment is defined as “all the ways of coming to conclusions about what has been perceived” [17]. It is further stated that if people differ systematically in what they perceive and in how they reach conclusions, then it is only reasonable for them to differ correspondingly in their interests, reactions, values, motivations, and skills [17]. The four dichotomies are:

--Favorite world: Extraversion or Introversion (E-I) are mutually complementary attitudes. “Extraverts” are oriented primarily toward the outer world focusing their perception and judgment on people and objects, while “introverts” are primarily oriented toward the inner world focusing their perception and judgment upon concepts and ideas.

--Information: Sensing or Intuition (S-N) are opposite ways of perceiving information, either sensing observable facts or happenings through the five senses, or interpreting and adding meaning, relationships, and possibilities.

--Decisions: Thinking or Feeling (T-F) are contrasting ways of judgment, either thought by looking at logic and consistency, or felt by looking at people and special circumstances.

--Structure: Judging or Perceiving (J-P) are processes used in dealing with the outer world (i.e.: the extraverted part of life). Judging uses either “thinking” or “feeling”, while perceiving uses either “sensing” or “intuition”.

One pole of each of the four preferences is preferred (dominant) over the other pole (auxiliary) and these preferences on each index are independent of preferences for the other three indices. Thus, the four indices yield sixteen possible combinations. The characteristics of each type follow from the dynamic interplay of these processes and attitudes [17]. Table 1 lists these personality types:

TABLE I
SIXTEEN PERSONALITY TYPES

ISTJ	ISFJ	INFJ	INTJ
ISTP	ISFP	INFP	INTP
ESTP	ESFP	ENFP	ENTP
ESTJ	ESFJ	ENFJ	ENTJ

Source: The Myers & Briggs Foundation [17]

According to Lacey [1], the ideal profile for a criminal mastermind is INTJ, a highly organized planner and capable leader. These types are rare in the general population, but are found in a few information technology directors. A lone fraudster, being a shy, analytic loner in good company would likely belong to the INTP type. MBTI can indicate who is likely to commit a fraud, but cannot explicitly say who will commit a fraud, thus should be used with caution for profiling user behaviors [1].

Although the incorporation of profiling techniques into information security has been suggested, criminal investigations is the prevailing area in the field of security where profiling is currently used. Thus, an understanding about criminal profiling will provide insight into profiling techniques which may be adaptable to information security.

B. *Criminal Profiling*

Criminal profiling is defined as an investigative approach based on the premise that the crime scene provides details about offense and offender [18]. It is used in homicide, sexual assault, arson, etc. Criminal profiling is also defined as the careful evaluation of physical evidence for systematically reconstructing the crime scene and developing a strategy to capture the offender, by weeding out suspects, developing investigative strategy, linking crimes and suspects, and assessing risk [19]. Based on the premise that “every criminal works to a certain set of values”, criminal profiling is used to classify behavioral patterns and predict the next move [20]. The developed offender description contains: psychological variables (personality traits, psychopathologies, and behavior patterns), and demographic variables (age, race, gender, emotional age, marital status, socioeconomic level, occupation, level of education, arrest and offense history, geographic location or residence relative to crime scene, etc.) [21]. Criminal profiling uses geographic and psychological typologies to create a profile that isolates offender characteristics [18]. Geographically-based techniques focus on location of crime scene to locate offender’s home base by mapping offense locations. Psychologically-based techniques compile psychological background using crime scene details and observable behaviors of offender’s traits. Behavior is interpreted from the presence or absence of forensic elements, offender’s behavioral choices, modus operandi, signature behaviors, knowledge of crime scene’s dynamics, etc. [18]. Turvey [22] states that inductive criminal profiling entails broad generalization and statistical reasoning and is thus subjective. On the other hand, deductive criminal profiling based on behavioral evidence analysis is preferred since it is a dynamic process which could be used to capture successful criminal whose methods either become more refined or deteriorate over time [22].

IV. PROPOSED SYSTEM

The system proposed through this research to achieve internal control of information and communication within an organization is explained in this section. This system addresses the threat of improper sharing of information, both intentional and unintentional, by authorized insiders, with outsiders or other insiders not authorized to access that information. Even though most systems acknowledge the importance of focusing on the human factor in information security, most currently available efforts focus on technological solutions only. Yet, people easily bypass technological controls and restrictions. Thus, this system proposes a mix of social and technological solutions by monitoring the level of observance of secure practices by the employees of an organization, creating user behavioral profiles based on this data along with background information and job details, identifying users who might be problematic in the future, and providing them with education and training in ISM.

Curtailing or limiting the web browsing capability of personal use can be detrimental to an employee’s productivity [1]. Yet, depending on the project(s) the employee is working on and the criticality of the business information the employee has to access, it is sometimes mandatory to restrict web browsing and access to the Internet in order to protect the security of the business information used for the project. In some instances, the clients themselves specifically request such restrictions. This system addresses this problem by providing two separate modes: the “strict” mode, which is the default mode, and the “relaxed” mode. During the “strict” mode:

- Only pre-specified programs and services are allowed (all others are denied).
- All activities are monitored.
- All activities are logged.
- All retrievals, printing and copying of information are logged and copies of files are tagged.
- Only work-related activities are allowed.
- No personal browsing, personal e-mails, or instant messaging, etc. are allowed.
- All information exchanges (e-mail contents, e-mail attachments, file-sharing, etc.) are recorded.

The “relaxed” mode must specifically be activated and these activation and deactivation times are logged and used for profiling and performance evaluations. During the “relaxed” mode:

- Personal browsing, personal e-mails, instant messaging, etc. are allowed.
- Personal activities are not monitored (to protect the user’s privacy).
- No access to work-related information (databases, etc.) is allowed.
- E-mail attachments and file sharing are recorded.
- Contents of excessively long e-mails are recorded.

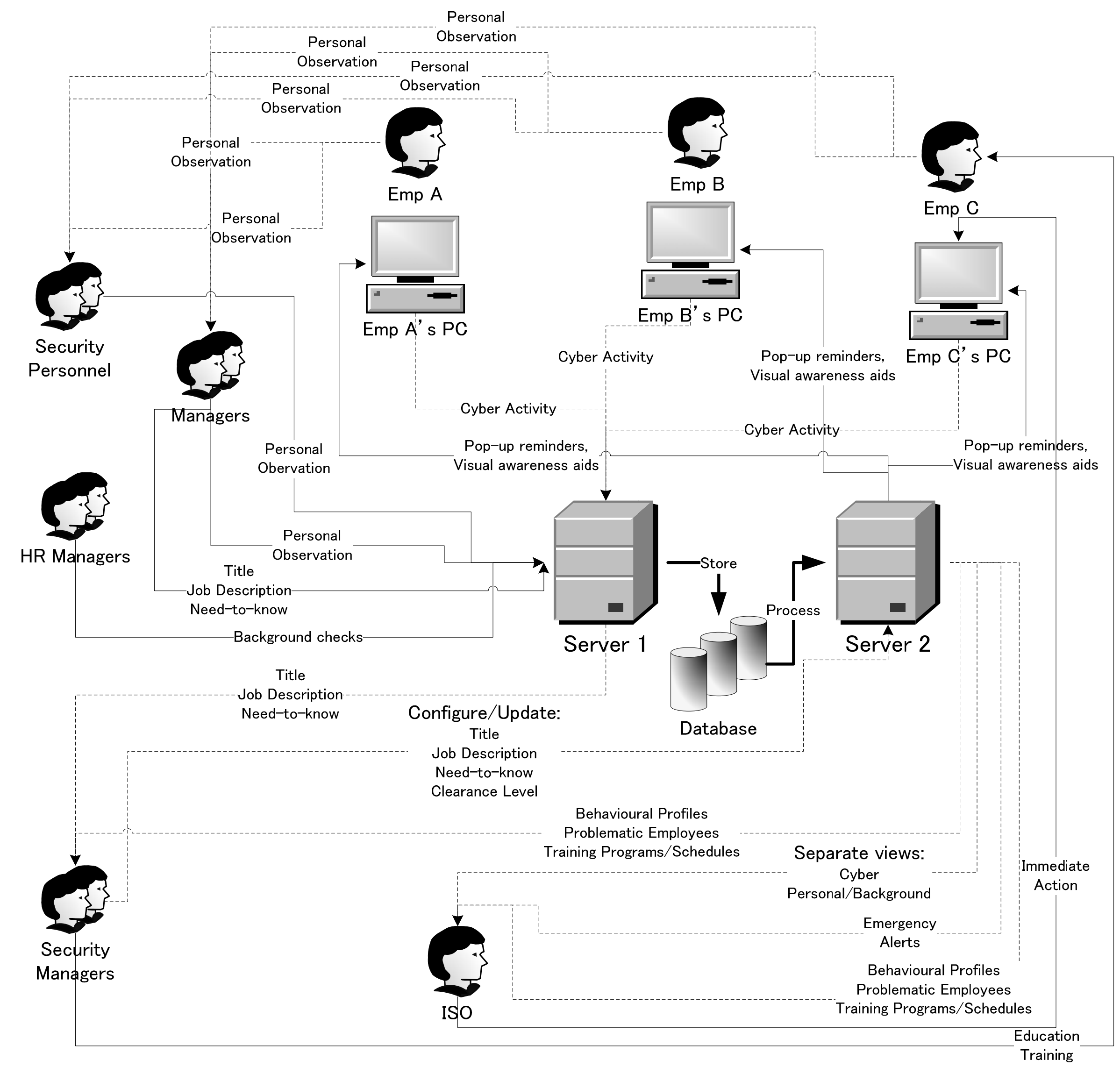

Fig. 1. Architectural design. This figure depicts the top-level architectural design of the proposed system.

The system will constantly monitor for extraordinary behavior:

- Excessive access to information, services, or systems
- Untimely access to information, services, or systems
- Access from remote terminals
- Trying to access data of a higher classification level than the user's security clearance level
- Trying to access data for which the user has no Need-to-Know according to the user's job description

Employees' level of observance of best practices will be monitored regularly in the following areas:

A. *Password Security Behavior:*

- Password strength (difficulty of remembering password, difficulty of guessing password, obviousness, etc.)
- Frequency of changing password
- Reuse of former passwords
- Whether the password is saved
- Whether the password is often mistyped
- Whether the password is often forgotten
- Time taken to type password
- Time taken to get used to typing a new password
- Whether the same password is shared across different applications
- Whether passwords are shared with others

B. *Data Backup Behavior:*

- Frequency of data backup (both company data and personal data, and both hard backup and soft backup)
- Whether the backup naming conventions are properly observed

C. *Data Sanitization Behavior:*

- Whether unnecessary copies of data are destroyed (both hard copies and soft copies)
- Sanitization of external storage media
- Whether access to personal storage media is controlled (whether they are lent to or freely accessible by others, whether they are used from different terminals, etc.)
- Use of others' storage media (whether they are scanned before using, whether they are sanitized before returning, etc.)
- Whether temp files, cookies, history, saved passwords, etc. are deleted

D. Network Security Behavior:

- Whether firewalls are enabled (whether they are relaxed to allow different applications access to the system, whether privilege is escalated to allow installation of software, whether escalated privileges are reset after installation of programs, etc.)
- Whether antivirus software is periodically updated
- Periodic computer scans
- Checking authenticity of websites, e-mail attachments, etc. before clicking on links or opening attachments
- Validating credentials of people before correspondence

E. Physical Security Behavior:

- Visibility of monitor
- Awareness of surrounding (whether others such as maintenance crew, janitors, etc. are around)
- Locking computer when leaving the desk
- Locking cupboards, desks, office, vehicle, etc.
- Whether confidential or personal items are left behind unattended (documents, computers, storage media, password hints, etc.)
- Whether personal items are shared with others
- Whether unknown items are used without validation
- Forgetting, lending or borrowing keys

Cyber activities of users such as password renewal frequency, reuse of former passwords, password strength, data backup frequency, etc., will be regularly monitored automatically by the system. Non-cyber activities such as whether the users leave confidential documents lying around, whether doors are locked, whether credentials are validated before revealing information to others, etc. will be monitored personally by their managers or the security personnel of the organization. Managers and security personnel may gather this information from what they notice during work hours or by performing a walk-through after office hours. Cyber activity monitored by the system will be stored separately, in parallel with other non-cyber activities monitored and inputted into the system by managers and security personnel.

The system will then create profiles for users based on behavioral patterns:

- Information from background checks before employment and periodically during employment are inputted to the system by human resource managers. These include: contact details, financial status and stability, number of dependents, educational level, criminal record, etc. This information will help in identifying users that might be enticed to reveal information for financial or career-wise incentives etc.
- Employee’s job description will be inputted or updated by his manager according to the project(s) the employee is currently working on. Responsibility entailing the job and the records of performance evaluations will be included. This information would help in identifying users that try to access information above their security clearance level or for which they do not have a Need-to-Know, and users that might be enticed to reveal information for career-wise incentives etc.
- Personal views about the behavior of employees will be inputted by the managers and security personnel. This information will help in identifying personality traits of employees, whether they feel isolated from their peers, whether they feel pressurized under competition, whether they can be easily enticed or tricked into revealing information, etc.
- This information, together with other cyber-activity related information automatically gathered by the system is used for profiling and for finding the behavioral types each of the employees belong to.

The resulting security behavioral profiles will include:

- The security consciousness of the employee
- The extent of understanding of the security policy by the employee
- The value given to ISM rules and procedures by the employee and the extent of adherence to policies
- How easily information is revealed to others
- How easily an employee can be enticed or tricked into revealing information to others
- Employee’s ambitiousness and drive to move ahead in his or her career
- Employee’s sociability, capability to work in a team and respect gained by peers
- The potential of an employee to intentionally or unintentionally reveal or improperly share confidential information with others
- Whether the employee has any motive or incentive (financial, career-wise, social, psychological or personal) to access unauthorized information or reveal information to others

Based on these behavioral profiles, the system will identify potential problematic employees and determine the level of security awareness, guidance, or training they should be given:

- Planned and scheduled awareness and training programs for identified potentially problematic users
- Randomly scheduled awareness and training programs for all users, periodically, as risk perception renewals to maintain the desired level of security awareness
- Depending on the extent of problematic behavior, awareness and training programs could range from pop-up notifications automatically handled by the system, to workshops conducted by external security professionals
- Real-time alerts sent to the information security officer (ISO) if extensively problematic behavior is detected, thus allowing the ISO to take necessary action against the employee
- Security managers and the ISO can request to view behavioral profiles of users in summarized, detailed or graphical form
- Training schedules for employees can also be viewed by the security managers and the ISO
- The ISO can additionally request separate views of personally inputted (non-cyber-activity-related) data and automatically monitored (cyber-activity-related) data and use his personal judgment to avoid any personal bias of managers or security personnel towards employees

Given below are some possible example scenarios of detecting problematic employees using this system:

--Employee A is a senior accountant in charge of handling employee salaries. She is financially well established with good academic and professional qualifications and is at the peak of her career. Yet, if a colleague asks to use her computer for some personal purpose, she provides them with her authentication information in order to help them. Employee A has no career-wise, personal, or financial motives for intentional violation of the company's information security. Yet, she can be easily tricked into revealing confidential information and thus, is an easy target of social engineering. She needs a security training workshop to make her understand the risks of a security breach, along with periodic automatic reminders of secure information sharing practices.

--Employee B is a software analyst and is in serious financial crisis. He tries to access employee salary information for which he has no Need-to-Know. Employee B may be trying to intentionally violate the confidentiality and integrity of the organization's salary information. The ISO must closely monitor his activities and de-escalate his privileges and security clearance to restrict access.

By allowing observable information about employees' behavior to be inputted personally by managers and security personnel, and through automatic monitoring of cyber-activities of employees, this system attempts to handle the human-related problem of improper information sharing using both technological and social information gathering methods. It also provides a mixture of technological and social solutions by means of automatic access control, logging, and risk perception renewals by the system, along with hands on security awareness and training workshops conducted by security professionals, and the allowing of the use of personal judgment by the ISO.

V. Summary and Further Work

The system proposed in this paper addresses the threat of intentional or unintentional sharing of information in an improper way, by authorized insiders with outsiders or other unauthorized insiders. It aims to achieve internal control of secure information and communication practices within an organization by monitoring the level of observance of best practices by its employees, and creating user behavioral profiles in order to identify employees who might potentially be a threat to the organization's information security. It then schedules necessary security awareness and training programs.

This working research is still underway and the proposed system is currently being developed by the authors. After implementation is completed the authors hope to deploy the system and evaluate the solution.

References

[1] D. Lacey, *Managing the Human Factor in Information Security: How to win over staff and influence business.* West Sussex, England: Wiley, 2009.

[2] J. A. Schweitzer, *Protecting Business Information*. Newton, MA: Butterworth-Heinemann, 1996.

[3] M. Bean, (2008, February). Human Error at the Centre of IT Security Breaches. Available: http://www.newhorizons.com/elevate/network%20defense%20contributed%20article.pdf

[4] E. Pronin, "Perception and misperception of bias in human judgement," *Journal of Trends in Cognitive Sciences*, vol. 11, pp. 37-43, 2006.

[5] B. Schneier, (2011, November). The psychology of security. Available: http://www.schneier.com/essay-155.html

[6] B. R. Williams, "Do it differently," *Journal of Information Systems Security Association*, vol 9 (5), p. 6, 2011.

[7] C. Vroom and R. von Solms, "Information security: Auditing the behaviour of the employee," *IFIP TC11 18th International Conf. on Information Security (SEC2003)*, Athens, Greece. In *Security and Privacy in the Age of Uncertainty,* D. Gritzalis, S. De Capitani di Vimercati, P. Samarati and S. Katsikas, Ed., Norwell, MA: Kluwer Academic Publishers, 2003, pp. 401-404.

[8] D. M. Lynch, (2012, August). Securing against insider attacks. *Information Security and Risk Management*, pp. 39-47. Available: http://www.csb.uncw.edu/people/ivancevichd/classes/MSA%20516/Supplemental%20Readings/Supplemental%20Reading%20for%20Wed,%2011-5/Insider%20Attacks.pdf

[9] R. A. Grimes, (2012, August). How to thwart employee cybercrime. *Insider Threat Deep Drive – Combating the Enemy Within, InfoWorld – Special Report*, pp. 2-7. Available: http://resources.idgenterprise.com/original/AST-0001528_insiderthreat_2_v1.pdf

[10] P. Ning, S. Jajodia and X. S. Wang, *Intrusion Detection in Distributed Systems – An Abstraction-Based Approach*. Norwell, MA: Kluwer Academic Publishers, 2003.

[11] A. Liu, C. Martin, T. Hetherington and S. Matzner, "A comparison of system call feature representations for insider threat detection," In *Proc. 2005 IEEE Workshop on Information Assurance, United States Military Academy*, West Point, NY, 2005.

[12] R. F. Mills, M. R. Grimaila, G. L. Peterson and J. W. Butts, "A scenario-based approach to mitigating the insider threat," *Journal of Information Systems Security Association,* vol. 9 (5), pp. 12-19, 2011.

[13] R. V. Sabett, "Have you seen the latest and greatest 'security game changer'?" *Journal of Information Systems Security Association,* vol. 9 (5), p. 5, 2011.

[14] T. R. Peltier, *Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL: Auerback Publications, 2002.

[15] J. J. Gonzalez and A. Sawicka, "A framework for human factors in information security," In *Proc. 2002 World Scientific and Engineering Academic Society International Conf. on Information Security,* Rio de Janeiro, 2002.

[16] K. Foley, "Maintaining a proactive and sustainable security program while hosting and processing personally identifiable information," *Journal of Information Systems Security Association,* vol. 9 (5), pp. 25-32, 2011.

[17] The Myers & Briggs Foundation, (2012, March). MBTI basics. Available: http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/

[18] T. M. Young and S. Varano, "Profiling pros and cons: an evaluation of contemporary criminal profiling methodologies," Final report – Honors Program, Northeastern Univ., Boston, MA, 2006.

[19] M. Thompson, (2012, April). An introduction to behavioural evidence analysis. Available: http://colbycriminaljustice.wikidot.com/criminal-profiling

[20] J. Claridge, (2012, April). Criminal profiling and its use in crime solving. Available: http://www.exploreforensics.co.uk/criminal-profiling-and-its-use-in-crime-solving.html

[21] L. Winerman, "Criminal profiling: the reality behind the myth," *American Psychological Association,* vol. 35 (7), pp. 66-69, 2004.

[22] B. Turvey, "Criminal profiling: an introduction to behavioural evidence analysis," *The American Journal of Psychiatry,* vol. 157, pp. 1532-1534, 2000.