Global Journal of human-social science: C
Sociology & Culture
Volume 14 Issue 1 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-460X & Print ISSN: 0975-587X

Internal Control of Information Sharing through User Security Behavioural Profiling

By Suchinthi Fernando & Takashi Yukawa
Nagaoka University of Technology, Japan

Abstract- This paper presents a workable solution to address the human-related information security problem of improper sharing of information by insiders with outsiders or unauthorized insiders. This system differs from most currently available information security solutions as in that, instead of relying solely on technological security measures it adapts a mixture of social and technological solutions. The presented system monitors users' security best practices and behavioural patterns and creates user security behavioural profiles and thus identifies users who might potentially pose threats to the organization's information security. The system then determines and schedules the security education and training to be given to these users.

Keywords: information security, human behaviour, personality type, profiling, social, technological, insider threat.

GJHSS-C Classification : FOR Code: 160899

Strictly as per the compliance and regulations of:

Internal Control of Information Sharing through User Security Behavioural Profiling

Suchinthi Fernando [α] & Takashi Yukawa [σ]

Abstract- This paper presents a workable solution to address the human-related information security problem of improper sharing of information by insiders with outsiders or unauthorized insiders. This system differs from most currently available information security solutions as in that, instead of relying solely on technological security measures it adapts a mixture of social and technological solutions. The presented system monitors users' security best practices and behavioural patterns and creates user security behavioural profiles and thus identifies users who might potentially pose threats to the organization's information security. The system then determines and schedules the security education and training to be given to these users.

Keywords: information security, human behaviour, personality type, profiling, social, technological, insider threat.

I. Introduction

As the importance of considering human resource security has become apparent (Asai, 2007), information security is no longer considered a purely technological matter.

Ensuring that access to information is strictly limited to the personnel who need to know it in order to perform their assigned tasks is mandatory to succeed in business (Schweitzer, 1996). Yet, as Bean (2008) states, most identified information security breaches occur because of human errors, resulting from the lack of proper knowledge and training, ignorance and failure to follow procedures. Thus, being the weakest link in the chain of security, people may unintentionally reveal confidential information to others. Schneier (2008) 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, such as social engineering, spear phishing or collusion from an insider, where people are tricked into revealing confidential information to others, and thus require a human element to be completed successfully (Williams, 2011).

With the inclusion of users with non-malicious intent, the percentage of insiders wittingly or unwittingly involved in an attack originating from the inside is said to be at least 60%-80% (Lynch, 2012; Grimes, 2012). An insider threat is defined as "trusted users with legitimate access abusing system privileges (Liu et al. 2005), or as "intentionally disruptive, unethical, or illegal behaviour enacted by individuals possessing substantial internal access to an organization's information assets" (Mills et al. 2011). Insider attacks are indistinguishable or difficult to distinguish from normal actions as inside attackers have authorization to access and use the system and these actions are less likely to differ from the norm (Liu et al. 2005).

Vroom and von Solms (2003) explain that physical, technical and operational controls are used to carry out effective information security, where the operational controls concern the behaviour and actions of the employees. Yet, even though information systems security auditing ensures that an organization's security policies, procedures and regulations are effective, the adherence of employees to these audited policies is simply assumed (Vroom and von Solms, 2003). Thus, 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. Although most technical security measures may be somewhat sufficient to keep outside attacks at bay, technical measures alone are clearly insufficient to ward off insider attacks, since, people may easily bypass these technological controls and restrictions such as access control by revealing their authentication information to others. Sabett (2011) states that security systems should be designed by accepting that the bad guys are already inside the system. Human behaviour, which is performed according to the personality of the individual, can be categorized (Vrooms and von Solms, 2003). Observable behaviours include cyber activities, which provide only 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 (Mills et al, 2011) or a "walkabout" after normal working hours to look for key indicators of information security awareness such as whether the offices, desks and cabinets are locked, workstations, information and recording media are secured, etc. (Peltier, 2002). Personnel may be categorized according to job category, job function, their knowledge about information processing and technology, system or

Author α: Doctoral student of the Knowledge Systems Laboratory Department of Information Science & Control Engineering, Nagaoka University of Technology, 1603-1 Kamitomiokamachi, Nagaoka, Niigata Japan. e-mail: s095191@stn.nagaokaut.ac.jp
Author σ: Professor, Department of Management & Information Systems Science, Nagaoka University of Technology, Japan.
e-mail: yukawa@vos.nagaokaut.ac.jp

application used, as well as level of awareness. Peltier (2002) further discusses the methods used to convey the awareness message, where he states that a hands-on approach would be an efficient method of training, while the best method for awareness is to watch a video on the subject. He also mentions the importance of an informed outsider presenting the message as opposed to a known messenger doing so, and further states that awareness programmes must be scheduled around the work patterns of the audience and that the mornings on Tuesdays, Wednesdays or Thursdays would be the best (Peltier, 2002). Gonzales and Sawicka (2002) state that if security measures stay above a certain threshold and the risk is kept below the accident zone, accidents will not normally happen. Typically, perceived risk and compliance with security measures gradually decline when accidents do not occur as a consequence of improved security. Thus, they recommend risk perception renewals in order to sustain an appropriate level of risk perception through properly scheduled interventions such as security training and awareness programmes (Gonzales and Sawicka, 2002). Foley (2011) lists the requirements for a proactive and sustainable security programme to be: preventive (credentialing and restricting access through authorization of identity, time, and place), detective (auditing, monitoring, and referrals to validate allegation), corrective (additional monitoring or auditing, updating credentials, access restriction, or access removal), and feedback (dynamic, reactive, and planned feedback and creating and implementing solutions).

The system presented through this research incorporates these suggestions by blending social and technological solutions to monitor cyber and non-cyber activities of users, detect patterns among these behaviours, and use this information together with background information and job details to create security behavioural profiles to identify users who might potentially be problematic. The system then determines the level of security education or guidance needed and thereby schedules and either conducts automatic security awareness programmes or informs management of training sessions to be conducted. In addition, the system also conducts periodic risk perception renewals in order to maintain the risk perception level within the appropriate limit.

II. Presented System

The system presented through this research to achieve internal control of information sharing is explained briefly in this section. The detailed explanation of this system is available in (Fernando and Yukawa, 2013).

Lacey (2009) has pointed out that curtailing or limiting the personal browsing ability of employees is detrimental to their productivity. Yet, depending on 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 of that particular 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, which needs to be specifically activated. Only pre-specified, work-related programs and services are allowed during the "strict" mode, and all activities are monitored and logged, while personal browsing, e-mails, or instant messaging, etc. are disallowed, and all information exchanges (e-mail contents, attachments, file-sharing, etc.) are recorded. During the "relaxed" mode, personal browsing, personal e-mails, instant messaging, etc., are allowed, and are not monitored to protect the user's privacy, while access to work-related information is disallowed. Fig. 1 depicts the top level architectural design of the system. This system constantly monitors for extraordinary behaviour: excessive or untimely access to information, services, or systems, access from remote terminals, attempts to access data of a higher classification level than the user's security clearance level, or data for which the user has no Need-to-Know according to their job description and the projects they are currently working on. Additionally, employees' observance of best practices is monitored regularly in the areas of password security behaviour, data backup behaviour, data sanitization behaviour, network security behaviour, and physical security behaviour.

Cyber activities of users such as password renewal frequency, reuse of former passwords, password strength, and 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, during or after work hours, by their managers or the security personnel of the organization. Information from background checks conducted before employment and periodically during employment is inputted to the system by human resource managers. These include: contact details, financial status and stability, number of dependents, education level, criminal record, etc. Employee's job description will be inputted or updated by their manager according to the project(s) they are working on. Responsibility entailing the job and the records of performance evaluations will be included. Together, this information will be used for profiling and for finding the behavioural types each of the employees belong to. The resulting security behavioural profiles will include the security consciousness of the employee, the extent of understanding and the value given to ISM rules and procedures, the extent of adherence to policies,

how easily an employee can be enticed or tricked into revealing information, employee's ambitiousness and drive to move ahead in their career, sociability, capability to work in a team, and respect gained by peers, the employee's potential to intentionally or unintentionally reveal or improperly share confidential information, and whether the employee has any motive or incentive (financial, career-wise, social, psychological, or personal) to access unauthorized information or improperly reveal information to others.

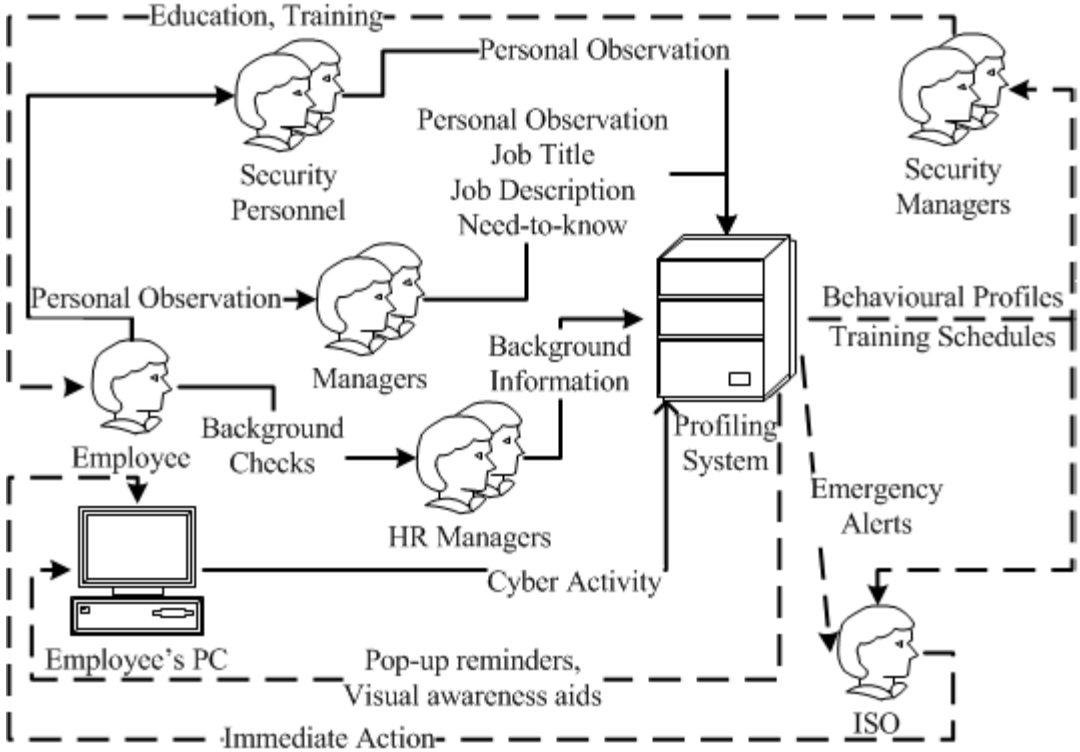

Figure 1 : Top-level architectural design.

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

- Planned and scheduled awareness and training programmes for identified potentially problematic users
- Randomly scheduled awareness and training programmes for all users, periodically, as risk perception renewals to maintain the desired level of security awareness
- Depending on the extent of problematic behaviour, awareness and training programmes could range from pop-up notifications automatically handled by the system, to workshops conducted by external security professionals
- Real-time alerts are sent to the information security officer (ISO) if extensively problematic behaviour is detected, thus allowing the ISO to take necessary immediate action
- Security managers and the ISO can request to view behavioural profiles of users in summarized, detailed, or graphical form, along with training schedules for employees
- 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 judgement to avoid any bias the managers or security personnel might have towards employees

III. Profiling

An insight into criminal investigations, the prevailing area in the field of security to use profiling, helps to better understand the security profiling techniques to be adapted for an information security system. Criminal profiling, used in homicide, sexual assault, arson, etc., is an investigative approach based on the premise that the crime scene provides details about offense and offender (Young and Varano, 2006) and is 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 an investigative strategy, linking crimes and suspects, and assessing risk (Thompson, 2011). Based on the premise that "every criminal works to a certain set of values", criminal profiling is used to classify behavioural patterns and predict the next move (Claridge, 2012). The developed

offender description contains: psychological variables (personality traits, psychopathologies, and behaviour patterns), and demographic variables (age, race, gender, emotional age, marital status, socioeconomic level, occupation, level of education, arrest and offense history, etc.) (Winerman, 2004). Criminal profiling uses geographic or psychological typologies to create a profile that isolates offender characteristics (Young and Varano, 2006). Of these, the presented system uses a psychologically-based technique, which compiles psychological background using observable behaviours of offender's traits. Behaviour is interpreted from the presence or absence of forensic elements, offender's behavioural choices, modus operandi, signature behaviours, knowledge of crime scene's dynamics, etc. (Young and Varano, 2006). Turvey (2000) states that inductive criminal profiling entails broad generalization and statistical reasoning and is thus subjective, whereas, deductive criminal profiling, based on behavioural evidence analysis, is a dynamic process which could be used to capture successful criminals whose methods either become more refined or deteriorate over time.

Lacey (2009) 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. Carl Jung's Theory of Psychological Types states that much seemingly random variation in human behaivour is actually quite orderly and consistent, being due to basic differences in the way individuals prefer to use their perception and judgement. According to the Myers & Briggs Foundation (n. d.), MBTI is based on Jung's ideas about perception and judgement and the attitudes in which these are used in different types of people to identify basic preferences of each of the four dichotomies specified or implicit in Jung's theory and to indentify and describe the sixteen distinctive personality types resulting from the interactions among these preferences. Perception is defined as "all the ways of becoming aware of things, people, happenings or ideas", while judgement is defined as "all the ways of coming to conclusions about what has been perceived". 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 (The Myers & Briggs Foundation, n.d.). The four dichotomies explained by the Myers & Briggs Foundation are summarized below:

- Favourite world: Extraversion or Introversion (E-I) are mutually complementary attitudes. Extraverts are oriented primarily toward the outer world focusing their perception and judgement on people and objects, while introverts are primarily oriented toward the inner world focusing their perception and judgement upon concepts and ideas.
- Information: Sensing or Intuition (S-N) are opposite ways of perceiving information, either focusing on basic information or interpreting and adding meaning. Sensing relies primarily upon the process of sensing, which reports observable facts or happenings through one or more of the five senses, while intuition relies upon the less obvious process of intuition, which reports meanings, relationships and/or possibilities that have been worked out beyond the reach of the conscious mind.
- Decisions: Thinking and Feeling (T-F) are contrasting ways of judgement, either looking at logic and consistency or looking at people and special circumstances. Thinking decides impersonally on the basis of logical consequences, while feeling decides primarily on the basis of personal or social value.
- Structure: Judging or Perceiving (J-P) are processes used in dealing with the outer world (the extraverted part of life). Judging uses a judgement process (thinking or feeling) and thus gets things decided, while perceiving uses a perceptive process (sensing or intuition) and stays open to new information and options.

One pole of each of the four preferences is dominant over the other (auxiliary) pole and these preferences on each index are independent of preferences for the other three indices, yielding sixteen possible combinations (The Myers & Briggs Foundation, n. d.). Table 1 lists these sixteen personality types.

Lacey (2009) emphasizes that MBTI can indicate who is likely to commit a fraud, but cannot explicitly say who will commit a fraud. In this research MBTI is used for validating the behaviours profiled by the presented system.

The behavioural characteristics shown in Table 2 are assumed for each of the following observable behavioural patterns when creating the user security behavioural profiles. The system allows these rules to be configured by the ISO to be aligned with the organization's business objectives. The default values are listed in Table 2.

"N" depicts not having the corresponding characteristic, while "Y" depicts having that characteristic. The characteristics not relevant to a corresponding observable behaviour are coloured in grey. Thus, according to the default values, the security behavioural profile for an employee who leaves items unattended, for example, will contain the characteristics of not being security conscious, easily revealing information, not valuing or understanding ISM rules, and having a potential for improper sharing of information.

IV. Behavioural Profile Viewing

To test this system, the authors created ten hypothetical test case scenarios as shown in Table 3. Table 4 displays the automatically monitored and

computed cyber activity for these ten hypothetical employees, while table 5 shows the personal views about non-cyber activities of the employees observed and inputted by managers and security personnel. The algorithms used for computing security behavioural profiles and for scheduling security awareness training are explained in detail in (Fernando and Yukawa, c.2014). Accordingly, the resulting security behavioural profile for employee Samantha Colt (Emp0008) in summarized form is: *"Information revealed easily. May have social incentives. Does not understand or value ISM rules. Not security conscious. May have financial motives. May have psychological motives and potential. Easy hack target. Suspicious behavior.",* while the detailed profile contains: *"Personal Views: Lends keycards and PINs. Does not understand or value ISM rules. Writes down passwords. Marital Status: Unmarried. Dependents: 1. Academic record: Computer Tech Certification. Financial Status: Low income. Criminal Record: Juvenile shoplifting. Password Strength: Weak. Password Modifying Frequency: Infrequent. Total Passwords: 2. Passwords reused over 10 times: 0. Passwords reused 6-9 times: 0. Passwords reused 3-5 times: 0. Passwords reused once or twice: 2. Attempts to access data over clearance level: 5. Attempts to access data without Need-to-Know: 5. Data Backup "Frequency: Infrequent"* Separate views of her behavioural profile, which can be viewed by the ISO, are displayed in Table 6, while fig. 2 depicts the graphical representation of her profile. The random schedule for periodic risk perception renewal is set in 4 weeks from the coming Tuesday for all employees. This security awareness training will likely consist of a pop-up presentation about security best practices followed by a questioning session to check the employees' understanding of security awareness.

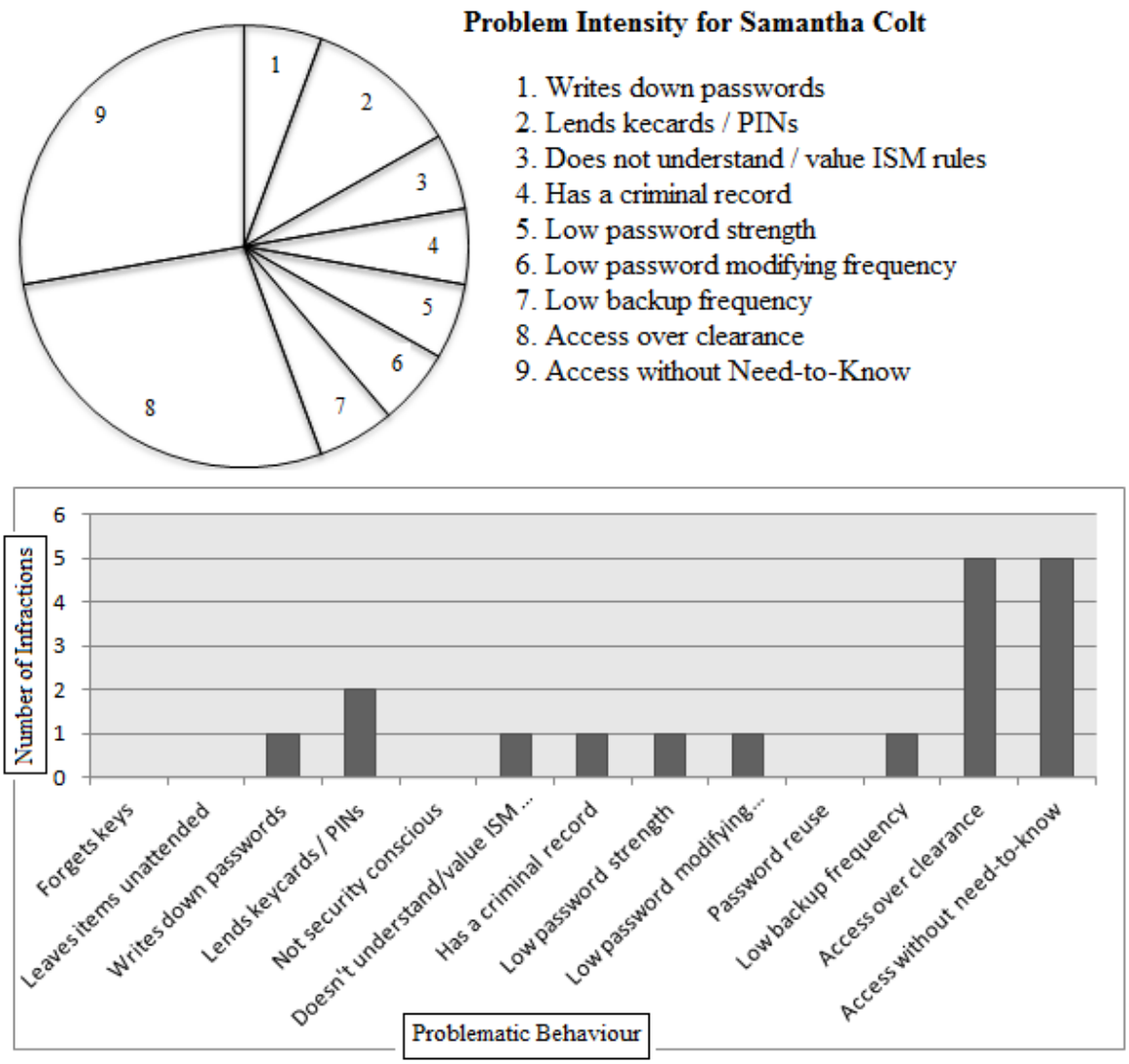

Figure 2 : Graphical View of the Security Behavioural Profile of Samantha Colt (Emp0008).

For employees who have a potential for improper information sharing, a hands-on security workshop conducted by external security professionals will be scheduled in 2 weeks from the coming Wednesday. If an employee has the potential for unauthorized access to information, the system will schedule a security seminar by security managers and legal officials in a week from the coming Wednesday. For employees who are deemed to have any kind of motive for engaging in improper information sharing or unauthorized access, the system will schedule closer inspection including background checks in 2 weeks from the coming Thursday. Thus, the training schedules computed on 30th September 2013 for an employee who requires all four types of security training will include a random awareness training on Tuesday, 29th October 2013, a security workshop on Wednesday, 16th October 2013, a security seminar on Wednesday, 9th October 2013, and a security inspection on Thursday, 17th October 2013. Fig. 3 displays these security training schedules for Samantha Colt (Emp0008) graphically on a calendar.

The summarized and graphical views of security behavioural profiles allow the ISO and the security managers to comprehend the major infractions by an employee at a glance, whereas, the detailed view provides more details about these infractions.

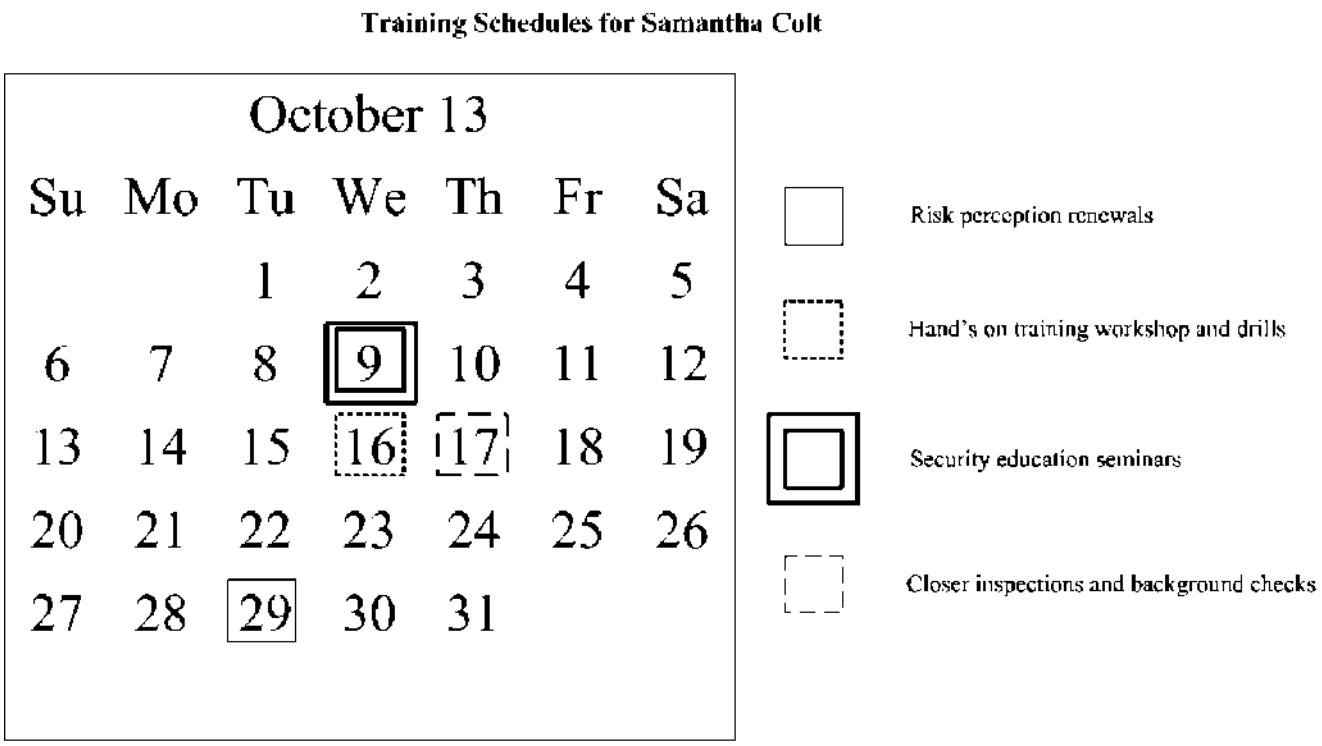

Figure 3 : Security Training Schedule for Samantha Colt (Emp0008).

Table 7 summarizes the resulting profiles obtained through the security behavioural profiling system on 30th September 2013. These results show that employees Monica White (Emp0002), Shaun Mills (Emp0003), Jacob Call (Emp0005), Samantha Colt (Emp0008) and Gavin Fields (Emp0009) have security behavioural flaws that could lead to information security problems along with motives or incentives, and thus need the hands-on training workshop, security educational seminar and closer inspection, along with the random security awareness. Employee Martha Hall (Emp0001), on the other hand, requires only the hands-on training workshop and closer inspection, along with the random security awareness programme. Employees John Flynn (Emp0004) and Faith Stellar (Emp0006) do not engage in any wrongful security behaviour, but their knowledge about computers and their background information show that they still require the security seminar showing the legal aspects of security violations as deterrence, along with closer inspection and the random security awareness. Employee Sarah Mason (Emp0010) is too new for the system to identify her security traits yet, but since she has already tried to access data without Need-to-Know once, and due to her background information, she requires the hands- on training workshop and security seminar, along with the random security awareness. Employee Claire McCormick (Emp0007), however, is an example of a case where the personal views of her manager might be biased. Her cyber activities and background information show that she does not engage in any wrongful security behaviour, but the personal views state otherwise. In this instance, the ISO can request separate views of her security profile, and upon seeing that the personal

observations by her manager contradict the rest of her security traits determined by the system, can use his or her own personal judgement to avoid any personal bias this employee's manager might have towards her, and thereby decide whether she requires the hands-on training workshop, or whether closer inspection and the random security awareness programme are sufficient. Table 8 depicts the MBTI personality types and resulting personalities of the employees as deemed true by the system according to the monitored cyber and non-cyber activities, and background information. The resulting personalities for each of the personality types listed in table 1 are adapted from the Myers & Briggs Foundation (n.d.). A "?" mark is used to depict an indeterminable dichotomy of personal preference, in which case the personality type and personality cannot be determined completely.

By comparing the data in table 8, concerning the personalities of the employees, with the resulting behavioural profiles in table 7, it can be seen that MBTI personality types and their resulting personalities match the behavioural profiles with sufficient accuracy. Thus, it is safe to assume that in the case the MBTI personality types of the employees of an organization are determined it could be used to provide insight into the behavioural patterns of the employees to a certain extent.

V. Conclusions and Future work

In conclusion, it can be stated that the system presented through this research provides a workable solution to achieve internal control of information sharing within an organization. By examining the automatically monitored cyber activities of the employees, their personally observed non-cyber activities, and their background information, the system compiles security behavioural profiles showing which of the employees could potentially engage in which wrongful activities that could present a threat to the organization's information security. Accordingly, the system also determines and schedules the level and type of security education and training to be given to each individual employee.

Through the results obtained by testing the system presented above with the hypothetical test cases, it can be stated that this system can be used for effective prediction of security infractions by employees within an organization to a certain extent.

By allowing observable information about employees' behaviour 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 judgement by the ISO. By providing a mix of social and technological solutions, the system enables an organization to provide a workable socio- technological solution to this human- related problem of information security and thereby overcomes the weaknesses of a purely technological solution.

Monitoring of employees' activities does, however, produce privacy implications. This system keeps such implications to a minimal by providing the two separate "strict" and "relaxed" modes to clearly distinguish the times when monitoring of activities will or will not be conducted.

By allowing the ISO to configure the security behavioural rules to be aligned with the business objectives of the organization, this system can be tailor-made to suit the specific requirements of the organization. Further, the summarized, detailed, graphical and separate views of security behavioural profiles and the graphical display of training schedules provide convenience to the ISO and security managers.

As future work, currently existing common algorithms could be reused with modifications and integrated to the implementation of this system to cover all the areas of monitoring of security behaviour proposed through this research. In addition, the system could be deployed and put to use on real people in order to obtain real test results to further evaluate the system's functionality.

References Références Referencias

1. Asai, T. (2007) Information security and business activities. Niigata, Japan: Kameda Book Service.
2. Schweitzer, J. A. (1996) Protecting business information. Newton, MA: Butterworth- Heinemann.
3. Bean, M. (2008) Human error at the centre of IT security breaches [Online]. Available from: http://www.newhorizons.xom/elevate/network%20 defense%20contributed%20article.pdf [Accessed 10th February 2008].
4. Schneier, B. (2008) the psychology of security [Online]. Available from: http://www. schneier.com/essay-155.html [Accessed 22nd November 2011].
5. Williams, B. R. (2011) do it differently. Journal of Information Systems Security Association, 9 (5), p. 6.
6. Lynch, D. M. (2006) Securing against insider attacks. Information Security and Risk Management, pp. 39-47 [Online]. Available from: http://www.csb. uncw.edu/people/ivancevichd/classes/MSA%20516/ Supplemental%20Readings/Supplemental%20Readi ng%20for%20Wed,%2011-5/Insider%20Attacks.pdf [Accessed 5th August 2012].

7. Grimes, R. A. (2010) How to thwart employee cybercrime. Insider Threat Deep Drive - Combating the Enemy Within, InfoWorld - Special Report, pp. 2-7 [Online]. Available from: http://resources.idgenterprise.com/original/AST-0001528_insiderthreat_2_v1.pdf [Accessed 5th August 2012].
8. Liu, A. et al. (2005) a comparison of system call feature representations for insider threat detection. In: Proceedings of the 2005 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.
9. Mills, R. F. et al. (2011) A scenario-based approach to mitigating the insider threat. Information Systems Security Association Journal, 9(5), pp. 12-19.
10. Vroom, C. and von Solms, R. (2003) Information Security: Auditing the behaviour of the employee. IFIP TC11 18th International Conference on Information Security (SEC2003), Athens, Greece. In: Gritzalis, D. et al. Security and Privacy in the Age of Uncertainty. Norwell, MA: Kluwer Academic Publishers, pp. 401-404.
11. Sabett, R. V. (2011) Have you seen the latest and greatest "security game changer"? Journal of Information Systems Security Association, 9(5), p. 5.
12. Peltier, T. R. (2002) Information security policies, procedures and standards: guidelines for effective information security management. Boca Raton, FL: Auerback Publications.
13. Gonzalez, J. J. and Sawicka, A. (2002) a framework for human factors in information security. In: Proceedings of 2002 World Scientific and Engineering Academic Society International Conference on Information Security, Rio de Janeiro.
14. Foley, K. (2011). Maintaining a proactive and sustainable security programme while hosting and processing personally identifiable information. Information Systems Security Association Journal, 9(5), pp. 25-32.
15. Fernando, S. A. and Yukawa, T. (2013) Internal control of secure information and communication practices through detection of user behavioural patterns. In: Proceedings of the World Congress on Engineering 2013, London, July 2013. Lecture Notes in Engineering and Computer Science, pp. 1248-1253.
16. Lacey, D. (2009) Managing the human factor in information security: how to win over staff and influence business. West Sussex, England: Wiley.
17. Young, T. M. and Varano, S. (2006) Profiling pros and cons: an evaluation of contemporary criminal profiling methodologies. Final report - Honours Programme, Northeastern University, Boston, MA.
18. Thompson, M. (2011) an introduction to behavioural evidence analysis [Online]. Available from: http://colbycriminaljustice.wikidot.com/criminal-profiling [Accessed 12th April 2012].
19. Claridge, J. (2012) Criminal profiling and its use in crime solving [Online]. Available from: http://www.exploreforensics.co.uk/criminal-profiling-and-its-use-in-crime-solving.html [Accessed 12th April 2012].
20. Winerman, L. (2004) Criminal profiling: the reality behind the myth. American Psychological Association, 35(7), pp. 66-69.
21. Turvey, B. (2000) Criminal profiling: an introduction to behavioural evidence analysis. The American Journal of Psychiatry, 157, pp. 1532-1534.
22. The Myers & Briggs Foundation (n. d.) MBTI basics [Online] The Myers & Briggs Foundation. Available from: http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/ [Accessed 15th March 2012].
23. Fernando, S. A. and Yukawa, T. (c.2014) Securing information sharing through user security behavioural profiling. In: Yang, G. C. et al. Transactions on Engineering Technologies: Special Volume of the World Congress on Engineering 2013, Springer, in print.

Table 1 : Sixteen Personality types (Source: The Myers & Briggs Foundation, n. d.)

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

Table 2 : Behavioural Characteristics for Observable Behavioural Patterns

Activity	Security Conscious	Reveals Information	Values/ Understands ISM Rules	Sociable	Ambitious	Technical Knowledge	Easy Hack Target	Suspicious Behaviour	Social Incentive	Career-wise Incentive	Personal Motive	Financial Motive	Psychological Motive	Improper Sharing Potential	Unauthorized Access Potential	Number
Personally Observed Non-Cyber Activities																
Forgets keys	N	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not forget keys	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Leaves items unattended	N	Y	N	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not leave items	Y	N	-	-	-	-	-	-	-	-	-	-	-	-	-	
Sociable	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	
Not sociable	-	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	
Ambitious	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	Y	
Not ambitious	-	-	-	-	N	-	-	-	-	-	-	-	-	-	-	
Writes down passwords	N	Y	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not write passwords	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Lends keys/PINs	-	Y	-	-	-	-	-	-	Y	-	-	-	-	Y	-	
Does not lend keys/PINs	-	N	-	-	-	-	-	-	-	-	-	-	-	-	-	
Security conscious	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Not security conscious	N	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Understands/values ISM rules	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	
Does not understand /value ISM rules	-	-	N	-	-	-	-	-	-	-	-	-	-	Y	-	
Background Information – Marital Status, Dependents, Academic Record, Financial Status, Criminal Record																
Married									-	-	-	-	-	Y	-	
Unmarried									Y	-	-	-	-	-	-	
Divorced									-	-	Y	-	-	-	-	
Widowed									-	-	-	-	-	-	-	
Dependents												Y				2
BS/MS in Computers						Y									Y	
No BA/BS/MS									Y							
Low income												Y				
Has criminal record													Y		Y	
Cyber Activities – Password Strength																
Very weak	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	
Weak	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	
Medium	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Strong	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Cyber Activities – Password Modification Frequency																
Infrequent	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	
Few times a year	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	
Monthly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Every 2 weeks	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Weekly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Excessively	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	Y	
Recent activity	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	Y	
Cyber Activities – Password Reuse																
Ten times or over	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	0
Six-to-nine times	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	0
Three-to-five times	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	1
Cyber Activities – Attempts to Access Data without Authorization																
Over clearance	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	Y	0
No need-to-know	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	Y	0
Cyber Activities – Backup Frequency																
Infrequent	N	-	N	-	-	-	-	-	-	-	-	-	-	-	-	
Weekly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Daily	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Excessively	-	-	-	-	Y	-	-	Y	-	-	-	-	-	Y	-	
Recent activity	-	-	-	-	-	-	-	Y	-	-	-	-	-	Y	-	

Table 3 : Hypothetical Employee Data

ID	Name	Designation	Marital Status	Dependents	Academic Record	Financial Status	Criminal Record
Emp0001	Martha Hall	Accountant	Unmarried	0	BA - Accounting	Steady income	None
Emp0002	Monica White	Software Engineer	Married	1	BS - Computer Science	Steady income	None
Emp0003	Shaun Mills	Computer Operator	Divorced	1	Computer Tech Certification	Low income	Juvenile breaking and entering
Emp0004	John Flynn	Software Engineer	Widowed	2	MS - Computer Engineering	Steady income	Teenaged hacking into Federal Database
Emp0005	Jacob Call	Computer Operator	Married	3	Computer Tech Certification	Low income	None
Emp0006	Faith Stellar	Software Engineer	Divorced	1	MS - Computer Engineering	Steady income	None
Emp0007	Clair McCormick	Accountant	Unmarried	0	BA - Accounting	Steady income	None
Emp0008	Samantha	Computer Operator	Unmarried	1	Computer Tech Certification	Low income	Juvenile shoplifting
Emp0009	Gavin Fields	Accountant	Divorced	3	BA - Accounting	Steady income	None
Emp0010	Sarah Mason	Software Engineer	Widowed	2	MS - Computer Engineering	Steady income	None

Table 4 : Cyber Activity

ID	Password Strength	Password Reuse	Password Modifying Frequency	Backup Frequency	Access Over Clearance	Access Without Need-to-Know
Emp0001	Medium	19_0_1_2_3	Every 2 weeks	Daily	0	0
Emp0002	Medium	12_0_0_2_5	Weekly	Excessive	0	2
Emp0003	Weak	20 _0 _1_2_ 2	Excessive	Excessive	2	1
Emp0004	Strong	13_0_0_0_12	Every 2 weeks	Weekly	0	0
Emp0005	Medium	3_0_0_0_3	Few times yearly	Infrequent	1	0
Emp0006	Strong	8_0_0_0_8	Monthly	Daily	0	0
Emp0007	Medium	7_0_0_1_4	Monthly	Weekly	0	0
Emp0008	Weak	2_0_0_0_2	Infrequent	Infrequent	5	5
Emp0009	Medium	18_0_0_3_2	Recent activity	Recent activity	2	3
Emp0010	Strong	3_0_0_0_3	Too new to determine	Too new to determine	0	1

Table 5 : Personal Views on Non-cyber Activity

ID	Manager's View	Security Personnel's View
Emp0001	Forgets keycards	Leaves items unattended
Emp0002	Sociable, ambitious	-
Emp0003	Writes down passwords, leaves items unattended	Forgets keycards
Emp0004	Security conscious, ambitious	-
Emp0005	Sociable, lends keycards and PINs	Forgets keycards
Emp0006	Security conscious, understands and values ISM rules,	-
Emp0007	Lends keycards and PINs, does not value ISM rules	-
Emp0008	Lends keycards and PINs, does not understand or value ISM	Lends keycards and PINs, writes down
Emp0009	Ambitious	-
Emp0010	-	-

Table 6 : Separate Views on Employee Samantha Colt's (Emp0008) Security Behaviour

View	Profile
Cyber Activities	Easy hack target. Not security conscious. Does not understand or value ISM rules. Suspicious behaviour.
Background Information	May have social incentives. May have financial incentives. May have psychological motives and potential.
Manager's View	Information revealed easily. May have social incentives. Does not understand or value ISM rules.
Security Personnel's View	Not security conscious. Information revealed easily. May have social incentives.

Table 7 : Computed Security Behavioural Profiles, Security Status, and Training Schedules

ID	Profile	Security Status	Random Schedule	Workshop Schedule	Seminar Schedule	Inspection Schedule
Emp0001	Not security conscious. Information revealed easily. Does not understand or value ISM rules. May have social incentives. Easy hack target.	Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	None	2013_10_17
Emp0002	Sociable. Ambitious. May have career-wise incentives. Has technical knowledge about computers. Not security conscious. Does not understand or value ISM rules. Easy hack target. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0003	Not security conscious. Information revealed easily. Does not understand or value ISM rules. May have personal motives. May have social incentives. May have financial motives. May have psychological motives and potential. Suspicious behaviour. Easy hack target. Ambitious.	Has unauthorized access potential. Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0004	Ambitious. May have career-wise incentives. Security conscious. Has technical knowledge about computers. May have psychological motives and potential.	Has unauthorized access potential. Has motives/ incentives.	2013_10_29	None	2013_10_9	2013_10_17
Emp0005	Sociable. Information revealed easily. May have social incentives. Not security conscious. May have financial motives. Does not understand or value ISM rules. Easy hack target. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0006	Ambitious. May have career-wise incentives. Security conscious. Understands and values ISM rules. May have personal motives. Has technical knowledge about computers.	Has unauthorized access potential. Has motives/ incentives.	2013_10_29	None	2013_10_9	2013_10_17
Emp0007	Information revealed easily. May have social incentives. Does not understand or value ISM rules.	Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	None	2013_10_17
Emp0008	Information revealed easily. May have social incentives. Does not understand or value ISM rules. Not security conscious. May have financial motives. May have psychological motives and potential. Easy hack target.	Has unauthorized access potential. Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0009	Ambitious. May have career-wise incentives. May have personal motives. May have financial motives. Suspicious behaviour. Not security conscious. Does not understand or value ISM rules. Easy hack target.	Has unauthorized access potential. Has improper sharing potential. Has motives/ incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0010	Has technical knowledge about computers. Does not understand or value ISM rules. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential.	2013_10_29	2013_10_16	2013_10_9	None

Table 8 : Computed Personality Types and Personalities

ID	Personality Type	Personality
Emp0001	?SF?	Cannot determine personality
Emp0002	IN?P	Cannot determine personality
Emp0003	ISFP	Friendly, sensitive, likes own space and own time, loyal, committed, dislikes conflicts, enjoys present moment.
Emp0004	INTP	Seeks explanations, theoretical, not sociable, focused, analytical.
Emp0005	ESFP	Outgoing, friendly, accepting, loves material comforts, sociable, realistic, spontaneous.
Emp0006	INTJ	Develops perspectives, achieves goals, sceptical, has high performance standards.
Emp0007	ESFP	Outgoing, friendly, accepting, loves material comforts, sociable, realistic, spontaneous.
Emp0008	?SFP	Cannot determine personality
Emp0009	I??P	Cannot determine personality
Emp0010	INTP	Seeks explanations, theoretical, not sociable, focused, analytical.