International Journal of Security and Its Applications
Vol. 12, No. 1 (2018), pp.37-46
http://dx.doi.org/10.14257/ijsia.2018.12.1.03

Mitigation Strategies for Unintentional Insider Threats on Information Leaks

Wan Basri Wan Ismail[1] and Maryati Yusof[2]

Faculty of Technology and Information Science, Universiti Kebangsaan Malaysia
[1]wanbasri@unisel.edu.my, [2]maryati.yusof@ukm.edu.my

Abstract

Information leakage is a major concern for many organizations. Information leakage becomes critical when the perpetrator is an insider. One often overlooked on the security breach that are caused by unintentional human behaviour in organizational daily activities. Human behaviour that poses a critical risk in organization includes human error, omitted security behaviour and the practice of security shadow IT. These unintentional acts are an important source of risk to information assets especially with the current challenges brought by the social media phenomena such as Bring Your Own Devices (BYOD) to office, and social engineering attacks. Technology alone cannot guarantee a secure environment for information assets. Appropriate risk analysis, monitoring and auditing of technology, organizational culture, people and procedures are crucial strategies in managing information security management. This paper aims to discuss human errors and behavioural activities in daily job activities that are exposed to current security breaches. The mitigation strategies for current threats posed by unintentional insider activities are also presented.

Keywords*: Unintentional Insider threat; omissive security behaviour; human behaviour; information leaks*

1. Introduction

Information systems user often engage in risky behaviour that threatens organizational security and integrity by exposing sensitive information. Most security breaches experienced by corporations are caused by insider threats [1]. Insider threats that could harm organizational information assets refer to individuals with access to privileges and facilities who can abuse these privileges on other services and resources [2], [3]. Nevertheless, not all insiders pose a threat to an organization. Insiders are defined as people who work with an organization or society. According to Sarkar [4], insiders are categorized into four main components, namely pure insiders (Internal staff), insider associates (Contractor, cleaner, security guard), affiliate insides (spouse, friends, client) and outside affiliates (ex-employee). Pure insiders refer to people who have access, knowledge and privilege to full or partial service of legitimate sources in an organization [5]. Meanwhile, Akunzada *et al*. [6] also defined pure insiders as administrators who possess complete privilege to perform essentially any operation on any critical system. This paper discussed human acts pertinent to unintentional insider threat activities in organizations. Unintentional insider threats have been identified through a review of the literature in the domain of information security management and information leaks in organizations.

Received (July 9, 2017), Review Result (December 15, 2017), Accepted (January 12, 2018)

ISSN: 1738-9976 IJSIA

2. Related Study

A. Unintentional Insider's Threat to Organization

Insider threat is divided into two categories, namely intentional and unintentional [7]–[10]. The classification of insider threat is shown in Figure 1. The intentional or malicious acts are usually triggered by tangible factors such as motive, opportunity and ability [11]–[13]. The motive-based act can be divided into four components, namely bad behaviour tendency (such as rule breaking), mental disorders (depression), personal factors (stress at work, passionate researcher) and the emotional state of the individual (hostile, revenge) [12]. Meanwhile, the opportunity-based factor is often associated with major causes of occurrence of insider threat activities [14]. These threats are associated with two activities. First, access to privileges and facilities granted to an individual to access a system, such as the super user administrator account [15]. Second, opportunity threats also arise through daily activities in an organization since valuable assets can be viewed, accessed and moved by insiders with the latest technology and innovation [13]. Meanwhile, the capacity factor represents the level of skill possessed by internal individuals who need to access and monitor the IT system.

Furthermore, unintentional insider threats could be classified into three types, namely human error [16], omissive security behaviour [17], [18] and shadow IT [19], [20]. Human error refers to carelessness or negligence such as accidental disclosure of information, loss of data storage, disposal of data that is not in accordance with procedures, use and maintenance. This includes of any information asset such as computers, password, network, storage, or any source that poses a threat to the organization. Human errors transpire due to the differences in skills, motivations, and knowledge among employees [21]. Human error also arises from work environments that are stressful to the employees, human interface machine issues, and other situational factors [22]. Figure 1 shows several activities caused by human errors. As stated by Liginlal *et al*. [22], the information processing stage constitutes the most cases of human errors.

Meanwhile, the scenario of employees who know how to protect their system but fail to do so is known as omissive security behaviour or the knowing-doing gap [23], [24]. It also refers to end-user who do not adhere to information security policies, for any reason. They know well about threats and countermeasures, but they do not do anything about it during events such as using social media for personal reasons at work, sending unencrypted confidential email, and do not prompt notification when their computers went missing. Other examples of omissive behaviour are shown in Figure 1. These omissive behaviour activities can seriously compromise the organization's information security posture and dangerously impact the availability, confidentiality and integrity of the information [24]. Moreover, there are several reasons for the knowing-doing gap; first, the inevitable loss of efficiency and productivity particularly when using automated and mandatory security measures. For instance, the system that restricts acceptable passwords for a designated range of characters or numeric or a firewall configuration that might affect the communication and encryption process that could impact productivity [18], [25]. The other reason why employees do not follow certain guidelines that relate to information security policies are due to unpredictable, rare and unusual circumstances. For example, in emergency cases, doctors and physicians might share their password when accessing the patient's record in the clinical system. Moreover, the activities of omissive security behaviour are also influenced by *workgroup norms*. It refers to people in the same workgroup, including supervisors and peers who have more influence on end-user behaviour [18]. In other words, they might be unaware or not concerned with behavioural ethics as long as they are doing the same thing as their peers. This means that the omissive security behaviour could frequently occur if no action is taken on the security violation.

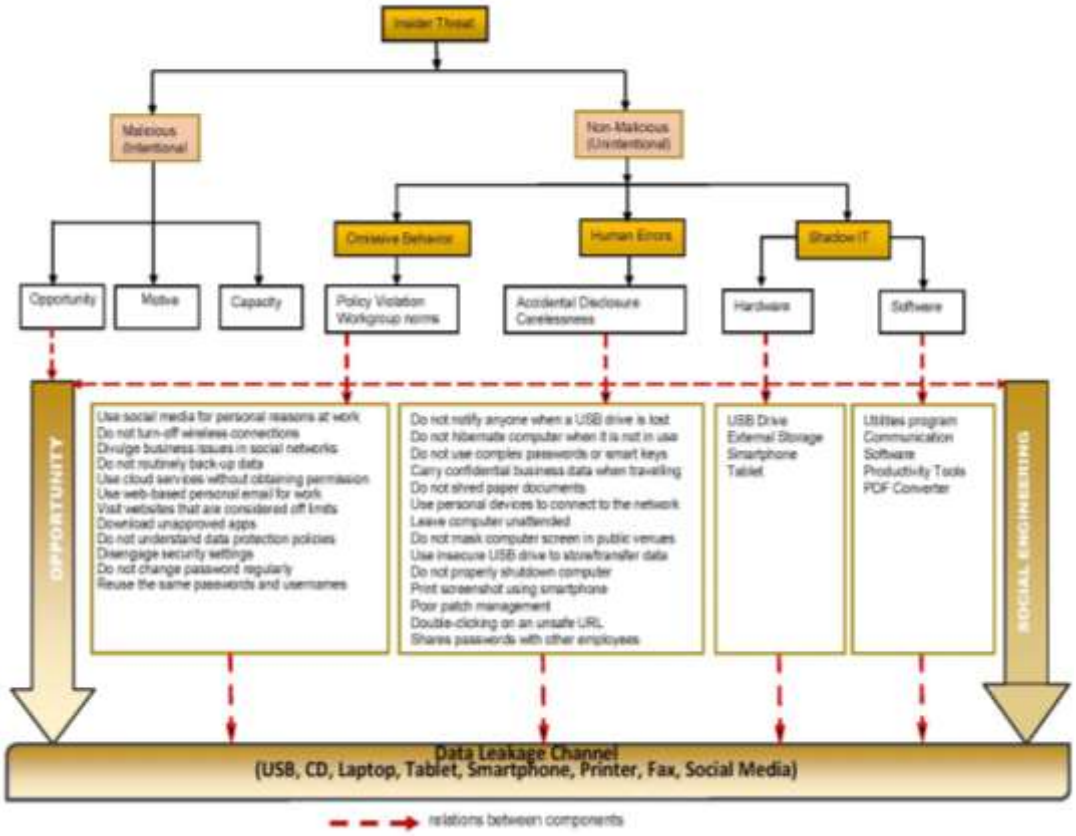

Figure 1. Classification of Insider Taxonomy and Threats Opportunities

The next category of unintentional threat is shadow IT or security shadow. The shadow IT phenomena is also considered as a security threat [26]. It refers to any software or hardware installed by employees without approval from IT department. Nevertheless, employees argue that these applications could increase job performance and the capability of fulfilling business needs [19]. It is an insider-threat, where a non-malicious insider (employee) installs disapproved software that strongly indicates a non-compliant behaviour towards an organization's information security policies [27]. Generally, the shadow IT defines the same autonomous developed systems, processes and organizational units developed by software and hardware without the awareness, acceptance, knowledge and support from the IT department [19]. The employee's act is considered as activities that they try to void of any malicious intentions [19]. Examples of shadow IT software are installed productivity software (*e.g.* Dropbox, Google apps), communication software (*e.g.* whatsapps desktop, IM, Skype), utility tools (*e.g.* CCleaner or WinZip), and PDF tools (*e.g.* PDF Creator, PDF Converter).

By installing these unapproved software, the risks presented by Malware are greatly increased and this directly affect data and information integrity. Unfortunately, most employees claim that these software are beneficial to their own and organizational productivity and as well as [19]. They also argued that they are not doing anything wrong and believe that the company will not sanction them for these 'small sins'. The study by Silic and Back [19] found that majority of employees are simply naive and lack the understanding of possible risks to organizational assets. Unfortunately, the restriction of shadow IT could be a big dilemma for a large organization, particularly when 20,000 employees demand shadow for IT software simultaneously. At the same time, IT is the enhancer and it

should thrive in the most efficient way to achieve business objectives [26]. The unintentional security behaviour might not be just an individual level phenomenon but more importantly a group level consensus [18]. Approaches like root cause analysis, effective policies and enforcement in organizations are crucial for handling these disruptions.

3. Information Leakage Challenges

Information leakage occurs when data is accessed from a database, in transit or when in use and shared over the phone, tablet, computer, USB, social media, email, CD or any new end-point technology [28]–[30]. Many human actions are affected by subjectivity when making decisions, such as processing, defining the secrecy level of data or assigning access rights to specific users [11]. However, the lack of self-awareness of the potential value of information that can be manipulated by other parties could pose a risk to the organization [31], [32]. This could happen when users physically copy or take screenshots of sensitive documents by using a cell phone camera [29]. The situation becomes critical if the information or sensitive data stored in the mobile phone is unintentionally accessed or viewed by their partners at home or close friends at the workplace. Furthermore, the new generation of employees are more technology savvy and demand flexibility and freedom when using their own devices, including personal computers, smartphones and personal tablet at work. Consequently, face-to-face communication, discussion in office or meetings will be decreased. This scenario will also increase the amount of data that need to be made available to co-workers through online channels. A recent survey on BYOD (bring your own device) revealed that out of the thousands of employees who responded, the majority used their personal mobile devices for work [33].

This number is expected to rise from 350 million in 2014 to 4 billion by the year 2017[33]. However, the major problem with BYOD, as described by Amigorena [34], guarantee for complete elimination of the security and privacy risks. These issues, synchronized with a survey by Partner [33], show that the main security concerns related to BYOD are data leakage (72%), unauthorized access to company data and systems (56%), users who download unsafe applications (54%) and malware issues (52%). All these risks have the potential to facilitate cybercriminals to breach secured systems in BYOD organizations. According to Markelj and Bernik [35], the use and usability of mobile devices is on the rise, as are the threats. However, threats become more complicated and increasing due to the ignorance of individuals and use of security solutions. The growing trend of BYOD usage and the use of online communication creates new attack vectors for social engineering. The Web 2.0 services such as Twitter, Facebook, and other social networking sites, e-mail use, Instant Messaging (IM) communication have become a part of our daily routine in private and business communications. At work, they share and transfer highly sensitive documents and information in cloud services with other virtual users.

In recent years, vulnerabilities in security related to online communication and data sharing channels have often been misused to leak sensitive information. These vulnerabilities are manipulated by social engineering [36]. Social engineering attacks refer to a multi-dimensional process that include physical, social and technical aspects. It also comes with different stages of the actual attack. For instance, current online applications sometimes request permission to access sensitive data on the user's device. If an attacker were to create such an application, he would obtain the information and use it as a starting point for a social engineering attack. The aforementioned leakage challenges and unintentional insider activities can be attributed to many factors such as risks behind Shadow IT, omissive security behaviour, high level of carelessness or negligent insider activities in daily activities at work. Data integrity and account information represents the biggest threat due to the increase in the use of BYOD and the unawareness of employees

to the possible risks when using social network applications. Employees, even they know about the risk, but they still continue with their behaviour. Hence, these weaknesses expose an 'opportunity' for perpetrators to commit the crime.

4. Mitigation Strategies for Information Leakage

There are various preventive measures used to prevent information leakages. According to Hunker and Probst [37], the prevention measures could be viewed from various aspects of sociology, psychology and organization. Soomro *et al*. [31] emphasised on management activities, particularly on the development and implementation of information security policies, awareness, compliance training, effective human resource development, IT infrastructure management, IT alignment and human resource management. Meanwhile, Lebek *et al*. [38] focused on the awareness of information security and the theory of human behaviour applied to information security, while Mills *et al*.[39] analysed the pattern of human behavioural activity. In addition, Alawneh and Abaddi [7] studied data flow factors, workflows, work plans, comforts and staff loads..

Figure 2 shows generic mitigation strategies focusing on unintentional threats such as omissive security behaviour, shadow IT and human error. There are four domains focused in this proposed security control, namely technology, organization, people and processes. Instead of classifying clustered and sub-groups of security control elements, this study proposed that the relationship between each sub-element in the security control are related, dependent and complement each other. The dotted and dashed line represent the relationship between monitoring processes including risk analysis and auditing are crucial elements for security metrics and auditing for certain sub-groups in the security control. Meanwhile, the dotted dash line show that each element is dependent and complements each other, such as the DLP (Data Leakage Prevention) system, which as a prevention tool, needs support and integrates with other detection solutions, such as APT (Advanced Persistent Threat) and IAM (Identity Access Management), to optimise its functions.

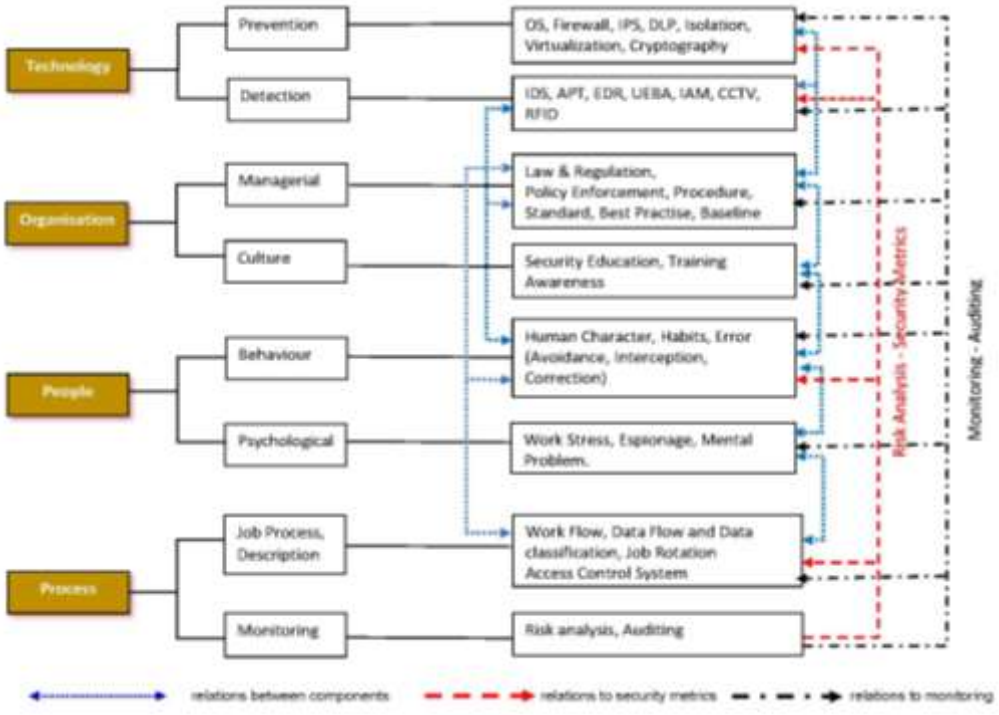

Figure 2. Generic Mitigation Strategies for Information Leaks

In Figure 2, technology or technical control consist of the prevention and detection methods. These technologies are incomplete without the enforcement from the management. Thus, policy enforcement, law and regulation as well as procedures are important in determining the technological deployment that needs to be synchronized and aligned with specific system security policies, baseline, standard, procedure and security Education Training Awareness (SETA). Top management also needs to change the organizational culture and working environment in such a way that it encourages compliance with IS security policies. They need to spread the message to their subordinates that compliance with IS security policies is everyone's work responsibility [20]. Thus, there are dotted line that are connected to the most of the sub-element groups in the security control.

SETA is capable of reducing errors among careless employees. Sometimes, errors occur when there is a lack of experience in security control and job processes. In a worst-case scenario, it could be a mismatch between the worker's mental state and the system's actual state. Thus, errors might arise from incorrect or incomplete knowledge, misuse of knowledge, application of faulty heuristics, and information overload [22]. The mismatch of worker's mental state and the system's state, faulty heuristics and information overload are related to human behaviour. Therefore, SETA is important in guiding and controlling human behaviour. In addition, human behaviour can be viewed and monitored by analysing user behaviour activities [39]. If user behaviour activities show abnormal behaviour compared to normal baseline behaviour, potential threats could occur. For example, when the logs history show the user login into system with abnormal from actual, the user profiling method can be used to observe user behaviour and forecast possible threats. Greitzer and Hohimer [40] added that incorporating psychosocial (mental problem, espionage, disgruntlement) data along with cyber data (user behaviour activities) into the behavioural analysis that offers an additional dimension to assess potential threats.

Moreover, the number of employees who commit omissive security behaviour, organizations should enforce security policies that warn employees of disciplinary action, including termination of employment [41]. A few studies have suggested that the role of formal and informal sanctions should be emphasized in organizations [42], [43]. A study on human behavioural characteristics and psychological assessment is crucial in understanding the employee's behavioural intentions to comply with security policies. According to Siponen and Vance [42], the Neutralization technique that focuses on perceived benefits of non-compliance, employee's moral beliefs, employee's perception of the severity of the consequences of noncompliance and their self-efficacy to comply with security policies are more useful in designing and reinforcing IS security policies. Since human psychology is related to human behaviour, it should be monitored by SETA and subjected to managerial enforcement.

Moreover, top management also needs to monitor and control the job process that is specifically related to confidential data. Data flow, data classification, access control and job rotation are important processes used to identify the root cause of why things go wrong and how to correct them [22]. For instance, there are technologies for error interception, such as artefacts that can be controlled by RFID tags through induced delays in the workflow. Meanwhile, the use of CCTV, periodical audit and isolating the location of certain information assets are the pre-eminent practical solutions used to reduce lost computer equipment and disposal of documents [22]. This shows that the job process is related to human behaviour, psychology and technical support.

Apart from job processes, monitoring processes are vital for ensuring reliable security controls. This is because IS security violations are not readily observable or objectively measurable. Human behaviour is difficult to study [18]. Thus, pro-active security metrics are essential in information security management especially to aid decision-making on security management and risk assessment [44]. The metrics

aims to provide risk scores so that different groups within the organization can set security targets and help identify acceptable risk levels [44]. Previously, most of the security metrics focused on technical aspects include access requests, intrusion attempts, virus logs, and traffic information. Nowadays, the introduction of the security metrics method allows for easier not only assessment of employee behaviour and integration of findings in security management. Therefore, this paper proposed that security metrics are not only related to technology, they are also associated to human characters, such as errors in intercepting and avoiding mistakes and negligent actions. The security metrics could also assist and reduce errors in the work flow and data flow processes. Besides security metrics, this study argued that all sub-security controls should be monitored and audited periodically, particularly those pertaining to technology, management, organizational culture, people, and job processes. The integration of all these actions enables a holistic information security management.

5. Conclusion

Unintentional insiders could cause security breaches and information leakage. Unintentional insiders pertinent to human factors and acts such as human errors, fatigue, risk perception and awareness, human limitation, biases, workload stress, personal traits, mood and mental disorder, age effects and cultural factors. However, this paper focuses on the risks of human behavioural activities in daily job activities that are exposed to recent security breaches. The use of current technologies such as BYOD and social media at the work place lead to the vulnerabilities and threats. The scenario is more critical if organizations are unable to protect and handle the omissive security behaviour, carelessness or human errors among their employees. It is not deniable that there are many security control assist in current information security management. For instance, in access control management, there are many access control models that based on the flexibility and environment of the system. These include the Situation-Based Access Control, Context Based Access Control, Activity Oriented Access Control, Owner-Based Access Control, Situation and Team-Based Access Control, Extended Attribute-Based Access Control, Workflow Based Access Control, Privacy Based Access Control, Spatial-Temporal Access Control and many more. However, the more security control is invented, the more security threats are created, especially with social engineering techniques and human weaknesses.

To reduce human behavioural risks, the development of security design principles based on employee behaviour and priorities is crucial for organizations to minimizing potential risks. Effective information security cannot be delivered only by perfecting the effectiveness of technical controls. Figure 2 shows the generic mitigation strategies that emphases on risks analysis and auditing on each components of security control domain. It is imperative to consider security systems and processes according to tasks, priorities and the user's level of understanding as well as each strategy and solution needs to be examined from the root cause. Moreover, these holistic approach should be integrated with the managerial control in organizations, people and processes.

References

[1] U. Franke and J. Brynielsson, "Cyber situational awareness – a systematic review of the literature", Comput. Secur, vol. 46, **(2014)**, p. 41.
[2] M. Jouini, L. B. A. Rabai and A. Ben Aissa, "Classification of Security Threats in Information Systems", in 5th International Conference on Ambient Systems, Networks and Technologies, vol. 32, **(2014)**, pp. 489–496.
[3] Z. M. Yusop and J. Abawajy, "Analysis of Insiders Attack Mitigation Strategies", Procedia - Soc. Behav. Sci., vol. 129, **(2014)**, pp. 581–591.
[4] K. R. Sarkar, "Assessing insider threats to information security using technical, behavioural and

organisational measures", Inf. Secur. Tech. Rep., vol. 15, no. 3, **(2010)**, pp. 112–133.
[5] M. Alawneh and I. M. Abbadi, "Defining and analyzing insiders and their threats in organizations", Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun., **(2011)**, pp. 785–794.
[6] J. Hunker and C. Probst, "Insiders and insider threats—an overview of definitions and mitigation techniques", J. Wirel. Mob. Networks, Ubiquitous, vol. 2, no. 1, **(2011)**, pp. 4–27.
[7] M. Alawneh and I. M. Abbadi, "Defining and analyzing insiders and their threats in organizations", Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2011, 8th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2011, 6th Int. Conf. FCST 2011, **(2011)**, pp. 785–794.
[8] B. Brock, "Detecting Insider Threats Using RADISH : A System for Real-Time Anomaly Detection in Heterogeneous Data Streams", IEEE Syst. J. , **(2017)**, pp. 1–12.
[9] H. G. Goldberg and W. T. Young, A. Memory, and T. E. Senator, "Explaining and aggregating anomalies to detect insider threats", Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2016–March, **(2016)**, pp. 2739–2748.
[10] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright and M. Whitty, "Understanding Insider Threat: A Framework for Characterising Attacks", 2014 IEEE Secur. Priv. Work., vol. 8533 LNCS, no. 4, **(2014)**, pp. 214–228.
[11] J. Eggenschwiler, I. Agrafiotis and J. R. Nurse, "Insider threat response and recovery strategies in financial services firms", Comput. Fraud Secur., vol. 2016, no. 11, **(2016)**, pp. 12–19.
[12] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis", Big Data Anal., vol. 1, no. 1, **(2016)**, p. 6.
[13] K. Padayachee, "An Assessment of Opportunity-ReducingTtechniques in Information Security : An insider Threat Perspective", Decis. Support Syst., **(2016)**.
[14] N. Elmrabit, S. Yang and L. Yang, "Insider Threats in Information Security", in 21st International Conference on Automation and Computing (ICAC), **(2015)**, pp. 1–6.
[15] I. Agrafiotis, J. R. C. Nurse, O. Buckley, P. Legg, S. Creese and M. Goldsmith, "Identifying attack patterns for insider threat detection", Comput. Fraud Secur, **(2015)**, pp. 9–17.
[16] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani and T. Herawan, "Information security conscious care behaviour formation in organizations", Comput. Secur., vol. 53, **(2015)**, pp. 65–78.
[17] M. Workman, W. H. Bommer and D. Straub, "Computers in Human Behavior Security lapses and the omission of information security measures : A threat control model and empirical test", vol. 24, **(2008)**, pp. 2799–2816.
[18] K. H. Guo, Y. Yuan, N. P. Archer and C. E. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", J. Manag. Inf. Syst., vol. 28, no. 2 **(2011)**, pp. 203–236,.
[19] M. Silic and A. Back, "Shadow IT - A view from behind the curtain", Comput. Secur., vol. 45, **(2014)**, pp. 274–283.
[20] I. Kirlappos, "Learning from' shadow security': understanding non-compliant behaviours to improve information security management", University College London, **(2016)**.
[21] D. Miyamoto and T. Takahashi, "Toward automated reduction of human errors based on cognitive analysis", in Proceedings - 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2013, **(2013)**, pp. 820–825.
[22] D. Liginlal, I. Sim and L. Khansa, "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management", Comput. Secur., vol. 28, no. 3–4, **(2009)**, pp. 215–228.
[23] K. H. Guo, "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis," Comput. Secur., no. 1, **(2012)**, pp. 1–10.
[24] J. Cox, "Information systems user security: A structured model of the knowing–doing gap", Comput. Human Behav., vol. 28, no. 5, **(2012)**, pp. 1849–1858.
[25] A. Ahmad, J. Hadgkiss and a. B. Ruighaver, "Incident response teams – Challenges in supporting the organisational security function", Comput. Secur., vol. 31, no. 5, **(2012)**, pp. 643–652.
[26] A. A. B. Györy, A. Cleven, F. Uebernickel and W. Brenner, "Exploring The Shadows: IT Governance Approaches To User-Driven Innovation", in European Conference of Information Systems, **(2012)**, p. 222.
[27] R. Willison and M. Warkentin, "RESEARCH C OMMENTARY BEYOND DETERRENCE : AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE", **(2013)**.
[28] R. Afreen, "Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges", Int. J. Emerg. Trends Technol. Comput. Sci., vol. 3, no. 1, **(2014)**, pp. 233–236.
[29] S. Aln and V. Muth, "A survey on Data Leakage Prevention System", J. Netw. Comput. Appl., vol. 62, **(2016)**, pp. 137–152.
[30] A. Hovav and F. F. Putri, "This is my device ! Why should I follow your rules ? Employees ' compliance with BYOD security policy", Pervasive Mob. Comput., **(2016)**.
[31] Z. A. Soomro, M. H. Shah and J. Ahmed, "Information security management needs more holistic approach : A literature review", Int. J. Inf. Manage., vol. 36, **(2016)**, pp. 215–225.
[32] Symantec, "Internet Security Threat Report", **(2016)**.
[33] G. Partner, "BYOD & Mobile Security: 2016 Spotlight Report", **(2016)**.

[34] F. Amigorena, "The threat from within : how to start taking internal security more seriously", Comput. Fraud Secur., no. July, **(2014)**, pp. 5–7.
[35] B. Markelj and I. Bernik, "Safe use of mobile devices arises from knowing the threats", J. Inf. Secur. Appl., vol. 20, **(2015)**, pp. 84–89.
[36] K. Krombholz, H. Hobel, M. Huber and E. Weippl, "Advanced Social Engineering Attacks", J. Infromation Secur. Appl., vol. 2, **(2014)**, pp. 113–122.
[37] J. Hunker and C. Probst, "Insiders and insider threats—an overview of definitions and mitigation techniques", J. Wirel. Mob. Networks, Ubiquitous, **(2011)**, pp. 4–27.
[38] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann and B. Hohler, "Employees' information security awareness and behavior: A literature review", in Proceedings of the Annual Hawaii International Conference on System Sciences, **(2013)**, pp. 2978–2987.
[39] J. U. Mills, S. M. F. Stuban and J. Dever, "Predict insider threats using human behaviors", IEEE Eng. Manag. Rev., vol. 45, no. 1, **(2017)**, pp. 39–48.
[40] F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks", J. Strateg. Secur., vol. 4, no. 2, **(2011)**, pp. 25–48.
[41] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who", Comput. Secur., vol. 61, **(2016)**, pp. 169–183.
[42] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations1", MIS Q., vol. 34, no. 3, **(2010)**, pp. 487–502.
[43] A. Vance and M. T. Siponen, "IS Security Policy Violations: A Rational Choice Perspective", J. Organ. End User Comput., vol. 1, no. 24, **(2012)**.
[44] M. E. Johnson and E. Goetz, "Embedding information security into the organization", IEEE Secur. Priv., vol. 5, no. 3, **(2007)**, pp. 16–24.

Authors

Wan Hassan Basri Wan Ismail, he is a lecturer at the Faculty of Communication, Visual Art and Computing, Universiti Selangor (UNISEL), Bestari Jaya Campus, Malaysia. He obtained his Master of Science in Information Technology from UiTM, Malaysia and Doctor of Education from UNISEL. Currently, he is PhD candidate at Faculty of Technology and Information Science, National University of Malaysia (UKM), Malaysia. His research interests include information security, management information systems and network security.

Maryati Mohd Yusof, she is an Associate Professor at the Faculty of Technology and Information Science, University Kebangsaan Malaysia (UKM). She obtained her Master of Science from UKM, Malaysia and Doctor of Philosophy from Brunel, West London. Her main research interests include Health Informatics, particularly Health Information Systems Evaluation, Information Systems Development and Management, Business Process Management, Human and Organizational issues in IS, Cybernetics, particularly the Viable System Model and Ontology. Her specialization areas are Information Systems Evaluation, Information Systems Adoption and Diffusion, Health Information Systems.

