HUMAN FACTORS IN INFORMATION LEAKAGE: MITIGATION STRATEGIES FOR INFORMATION SHARING INTEGRITY

Structured Abstract

Purpose – The purpose of this paper is to explore the human factors triggering information leakage and investigate how companies mitigate insider threat for information sharing integrity.

Design/methodology/approach – The methodology employed is multiple case studies approach with in-depth interviews with five Multinational Enterprises/Multinational Corporations.

Findings – The findings reveal that information leakage can be approached with human governance mechanism such as organizational ethical climate and information security culture. Besides, higher frequency of leakages negatively affects information sharing integrity. Moreover, this paper also contributes to a research framework which could be a guide to overcome information leakage issue in information sharing.

Research limitations/implications – The current study involved MNC/MNEs operating in Malaysia while companies in other countries may have different ethical climate and information sharing culture. Thus, for future research, it will be good to replicate the study in a larger geographic region to verify the findings and insights of this research.

Practical implications – This research contributes to the industry and business that are striving towards solving the mounting problem of information leakage by raising awareness of human factors and to take appropriate mitigating governance strategies to pre-empt information leakage. This paper also contributes to a novel theoretical model that characterizes the iniquities of humans in sharing information, and suggests measures which could be a guide to avert disruptive leakages.

Originality/value – This paper is likely an unprecedented research in moulding human governance in the domain of information sharing and its Achilles' heel which is information leakage.

Keywords information leakage, organizational ethical climate, information security culture, information sharing, human governance

Paper type Research paper

1. Introduction

Advocates of information sharing had highlighted the potential benefits of using valuable information to improve overall organization performance (Fawcett, Osterhaus, Magnan, Brau, & McCarter, 2007; Kembro, Näslund, & Olhager, 2017). Information sharing is instrumental to foster collaboration and strengthen relationships among employees within an organization and across organizations with business partners (Lee & Whang, 2000). However, the advantages of information sharing can only be realized when the information shared

between the sender and the receiver is integral, wholesome and undistorted (Durugbo, Tiwari, & Alcock, 2014; Kwon & Suh, 2005). In other words, the value of the information shared remains intact and uncontaminated. In many cases, inaccurate or distorted information create chaos and disruption to the organization (Cannella, Framinan, Bruccoleri, Barbosa-Póvoa, & Relvas, 2015; Dai, Li, Yan, & Zhou, 2016; Kwak & Gavirneni, 2015). The fearful cause of information inaccuracy and distortion in information sharing is internal information leakage.

Many information sharing specialists believe that promoting technology to protect information against external attacks is an important method for making information sharing effective within organizations (Stoneburner, Goguen, Feringa, 2002; Sumner, Cantiello, Cortelyou-Ward, & Noblin, 2012). Surprisingly, although organizations always have been concerned about vulnerability to external threats, recent industry research indicates that a substantial amount of information leakage incidents actually originated from within the organization (Padayachee, 2016; Stanton et al., 2005). This is copiously supported by the Global Data Leakage Report 2016 of InfoWatch. Its latest issue of information leakage in 2016 shows that among the data leaks logged, 38.2% of the cases were triggered by external attacks, while 61.8% were caused by internal offenders (InfoWatch, 2016). These insider leakages are major concerns and constitute the primary attention of this research.

Information leakage refers to the act of intentional or unintentional disclosure of information to an unauthorized party (Anand and Goyal, 2009). Practically all companies are familiar to insiders posing risks due to their legitimate access to their organizations' facilities, assets and valuable information (Colwill, 2009; Hunker & Probst, 2011; Magklaras & Furnell, 2005). These insiders will likely know how to achieve the greatest impact while leaving behind little or no evidence (Colwill, 2009). These harmful loss and disclosures of business information are cited in business reports; and industry experiences have shown information leakage propagated by authorized user or insider threats are continually succeeding in harming organizations (Huth, Chadwick, Claycomb, & You, 2013). Therefore, insiders are among the greatest threat to the organization and insider leakage should be curbed if organizations want to gain competitive advantage through information sharing (Huong Tran, Childerhouse, & Deakins, 2016; Tan, Wong, & Chung, 2016; Zhang, Cao, Wang, & Zeng, 2012).

This study is important because the protection of confidential data against leakage is a growing concern going by the leakage statistics (InfoWatch, 2016). Apparently, the traditional way of protection using information security policies and conventional security mechanisms

such as firewalls, virtual private networks and intrusion detection systems continue to succumb to the exploits of insiders and outsiders alike (Alneyadi et al., 2016; InfoWatch 2016). Regrettably, these mechanisms lack proactiveness in protecting confidential data.

We posit that the inherent complexities of the insider threat impacting information leakage and the integrity of information sharing call for an examination of human factors. Thus, the overarching goal of this research is to investigate how companies could mitigate leakage caused by insider attacks in information sharing. Specifically, we wish to address the following research questions i.e. *RQ1: Why does information leakage happen? RQ2: How could information leakage impact information sharing integrity? RQ3: How could information leakage be mitigated?* The findings from this study will enable managers to make better-informed decisions to help them develop appropriate mitigation and governance strategies in order to maintain the consistency, accuracy and reliability information in their organizations (Nayar, 2004).

The exploratory nature of this study dictated that a qualitative, multiple case study approach should be adopted. The study involved a total of five multinational companies predominantly in the manufacturing sector. Semi-structured interviews together with secondary data source were used to capture valuable contextual information regarding the history and characteristics of each case company and its information exchange process. Interviews with representatives of the companies were also carried out to enable the researchers to gain deeper insights into the mitigation strategies for leakages to achieve information sharing integrity. This paper will proceed as follows. In the next section of the study, we review the literature of human factors and information leakage. Section 3 describes the research context, the data collection procedure and methodology. Section 4 details the data analysis and presents the results. Section 5 provides the discussion. Section 6 provides the managerial implications and proposed framework. Lastly Section 7 concludes the study.

2. Literature Review

Information leakage could occur in transit, in use and at rest (Alneyadi et al, 2016; Orgill et al., 2004). (See Fig. 1). Employees' actions and behaviors are especially important in information security as almost all information security solutions rely on the human element to a large degree. This could be understood from the "in use" stage where humans interface with the hardware such as computer terminals. The "in-use" stage interacts or connects with the "in transit" (cloud/internet) and also with the "at rest" where data is stored (Alneyadi et al, 2016).

The authorized user could access the internet/intranet and database to retrieve or copy information, or the unauthorized user could hack into them. Some devices and channels which could facilitate information leakage are the laptop, fax, tablet and smartphone, email, USB and the printer (Olzark, 2010). Noting users at the human computer interface could extract or steal information and share with unauthorized recipients, the discussion on human factors will be first discussed followed by unintentional and intentional leakages.

INSERT FIGURE 1 ABOUT HERE

2.1 Human factors

As described in the preceding section, in today's information society, the use of information technology (IT) is designed with the human-computer interface. This facilitates easy access to data storage for both proper and unethical purposes. These unethical uses of IT are easily committed by insiders (Crossler et al., 2013) often deliberately, and with malicious intent posing a major security threat (Haines and Leonard, 2007; Liang and Xue, 2010). Some examples of insider information leakage are the theft of personally identifiable information to commit fraud, theft of intellectual property, or for an insider to pass sensitive or classified information to unauthorized third parties (Greitzer & Frincke, 2010; Huth et al., 2013). These thefts and leakages are intentional and malicious. Da Veiga and Eloff (2010) correctly note that "an organisation's approach to information security should focus on employee [unethical] behavior." Underpinning the gravity of this unethical/immoral use of computers and information system (Kajzer et al., 2014) is "people could be the weakest link in IS security" (Cheng et al., 2013). This observation "has the greatest potential for loss and damage to the employer" (Willison et al., 2013). Following this, the converse is that the major obstacle to achieve information security in an organization is insider actions and behavior when they handle information (Okere et al., 2012). This is verified by the results of studies which conclude that insiders pose a threat to information security (Da Veiga & Eloff, 2010; Omar, 2015; Rhee etal., 2009; Stanton et al., 2005). Intuitively, insider threats are rightly attributed to the human-computer interface since they have authorized or unauthorized access. In addition, poor insider attitude and lack of awareness of security issues are also among the most significant contributors to security incidents (Endsley, 1995; Greitzer et al., 2014). For these, a key tool is to create security awareness to make insiders more aware of any significant risks lurking in the

company enabling them to act to protect information assets (AlHogail & Mirza, 2014; Da Veiga & Eloff, 2010).

Traditionally, organizations have paid considerable attention to the security of physical assets but largely ignored insiders who should learn appropriate and acceptable human behaviors for information asset security (Tseng & Fan, 2011). This ignorance could have humans practically failed to safeguard their companies' information assets (InfoWatch, 2016) resulting in leakage scandals. One common thread in such ethical scandals is the insider ex-post incentives offered by external parties (Tan et al., 2016). These insiders are influenced by competitors or other parties to intentionally act out disruptive, unethical or illegal behavior which compromises confidential information to achieve personal gains This particular behavior of leaking organization information to achieve personal gains is devious and threatens the well-being of an organization (Omar, 2015). It is also an unethical act that violates organization norms, formal or informal organizational policies, rules, and procedures (Robinson & Bennett, 1995). Therefore, ethical issues on the protection of information assets should deserve more attention and will constitute a major topic in information sharing (Da Veiga & Eloff, 2010).

The issue of human factors in information leakage is crucial especially in today's business digital world where information access and sharing are unavoidable in daily activities. Unfortunately, organizations are still not absolutely clear about human factors triggering intentional and unintentional leakage causing information sharing interruptions (disruptions) as there is sparse research in human factors. Some psychosocial indicators that are considered indications that an individual is a potentially malicious insider are disgruntlement, disagreeing with feedback, anger, disengagement, disregard for authority and performance issues (Greitzer & Frincke, 2010). In addition, information leakage could also refer to inadvertent information loss when forgetting to change password, failing to log off before leaving workplace, or carelessly discarding sensitive information rather than shredding it (McCormick, 2008; Warkentin & Willison, 2009). Oddly, information leakages may benefit some business operations. For instance, firms allow for voluntary information spillovers regarding an innovative product or process in order to accelerate the arrival date of the new inventions (Harhoff et al., 2003). Although information leakage or spillover may benefit from the increase in diffusion via a number of effects, leaked proprietary information may well flow outside the borders of any organizations in an uncontrollable, unwanted, and even harmful manner (Ritala et al., 2015) to allow competitors to similarly introduce their new products.

Regardless of the leakage type and motivation, the impact of these insider actions could precipitate in financial loss, disruption to the organization, loss of reputation, and long-term impact on organizational culture. Therefore, any impact may not depend on motivation because an innocent act of unintentional leakage can have as devastating an effect as a maliciously motivated attack (Hunker & Probst, 2011). The goal may therefore be to avoid catastrophic consequences regardless of the motivation (Hunker & Probst, 2011). With information leakage bringing more harm than good, it is counterproductive work behavior (Marcus et al., 2016) and could be dealt with mitigation techniques (Hunker & Probst, 2011).

Today, insiders who want to leak confidential or proprietary information may not need a great deal of specific knowledge of the information. Gigabytes or more of information can be exfiltrated or duplicated using various means including email, instant messaging, thumb drives and other modern information technology tools (Greitzer & Hohimer, 2011). Indeed, the only way to be proactive is analysis of insider behavior in order to recognize signs and precursors of the potential insider threat activity (Greitzer & Frincke, 2010). This is often evident in behavior prior to execution of the crime. However, sometimes it can be difficult to separate "acceptable" insider behavior from "unacceptable" behavior (Hunker & Probst, 2011).

Recognizing insider threats as human behavior deviance is an important starting point to control information leakages in addition to existing technical measures. The insider threat is revealed when human behaviors deviate from compliance with established policies or normal standards of conduct regardless of whether they are caused by ignorance, malice or disregard (Greitzer & Hohimer, 2011; Greitzer et al., 2008). Broadly, the act of leaking information is classified as an undesirable behavior by employees who share information for whatever reason which a company would rather protect (Ritala et al., 2015). Human behavior can wreak havoc on information sharing through intentional or unintentional abuse in the information sharing process because it could cause loss of information value to both the giving and recipient company in the supply chain information sharing. Identifying human factors of insider threats is thus necessary to mitigate information leakage. Therefore, it is timely for academics and managers to search for appropriate mitigation strategies to reduce information leakage effects in order to attain information sharing integrity.

2.2 Intentional leakage

A general overview of intentional leakage (IL) is a negative and deviant workplace behavior (Dimotakis et al., 2008; Robinson & Bennett, 1995) and is counterproductive to

desired work behaviour (Gruys & Sackett, 2003). Intentional implies premeditated, conscious and willful decision of an insider to harm the business operations of a company (Guo et al., 2011) while leakage connotes the prohibition of revealing critical information to an unauthorized entity (Ritala et al., 2015; Tan et al., 2016). Such occurrences stem from different motivations as described in the preceding section. This could happen when insiders are offered incentives to do so (i.e., to leak the organization's confidential information for pecuniary interests) or it could be a personal vendetta against the company (Nishat Faisal et al., 2007). Other reasons include "innocent action", "fun", "technical challenge", "criminal intentions", and "espionage", or a combination of each of these factors. (Hunker & Probst, 2011).

In behavioral psychology, the outcome from the act of malicious insider who exploits information for personal gains is intentional leakage (Warkentin & Willison, 2009). For instance, an insider primarily motivated by personal financial gain could intentionally disclose confidential information or misuse authorized access to steal and sell data (Cappelli et al., 2009). This behavior of malicious insiders in leaking information intentionally could be explained by the theory of human behaviorism (Nurse et al., 2014). This theory explains incentives could be internal (intrinsic) or external (extrinsic) and drive the pattern of human motivations. Intrinsic factor (e.g. employer's recognition) can motivate employees to exhibit good conduct during work but if the extrinsic factor (e.g. money and non-financial incentives offered by competitors and outsiders) overwhelms the effect of intrinsic, then it will cause behavioral change of insiders. The overpowering extrinsic factors would lure insiders to consciously violate organization norms and tend to commit evil acts to threaten the well-being of an organization (Sackett and DeVore, 2001). These evil acts cover a broad range of discrete activities e.g. (1) theft, (2) destruction of property, (3) misuse of information, (4) unethical decision making, and (5) workplace retaliation (Warkentin & Willison, 2009; Marcus et al., 2016). This explains external incentives could cause insiders to leak information when given sufficient financial and nonfinancial rewards.

Noting the above, the risks or danger signals associated with insiders who are threats to organization to leak information should be closely monitored and addressed. The risks from intentional human (malicious insiders) activity are especially dangerous to confidential information assets of organization (Hunker & Probst, 2011; Omar, 2015). This is because a malicious insider has the potential to cause more damage to company information infrastructures (Cappelli et al., 2012). Malicious insiders are trusted agents who have legitimate and privileged access to facilities and resources, and possess SWOT (strengths, weaknesses,

opportunities and threats) knowledge of the organization and its processes and know the location of critical or valuable information assets. This knowledge empowers insiders how, when and where to attack and cover their trails (Colwill, 2009; Hoecht & Trott, 2006; Warkentin & Willison, 2009; Huth et al., 2013). Hence, armed with ample opportunities, they can exploit their positions to steal information and leak them to an unauthorized third party making these insiders worrisome liabilities to the organizations (Hoecht & Trott, 2006) which could cause their organizations to lose competitive advantage.

Intentional leakage cause by frustration, personal vendetta, dislike of authority and inclination for revenge (Moore et al., 2009; Colwill, 2009) could also explain their effects which produce disequilibrium in human behaviorism. The unamicable situations in the work environment would infuse a negative driving force (disincentives) to the insiders and caused them to behave in a negative way. Engulfed with feelings of unhappiness, unfairness and resentment in their job, these tipping points would invoke a change in psychological state and attitudes to trigger attacks on selected assets and purposefully exposing critical business information to outsiders, third parties or new companies (Nurse et al., 2014). All these actions by the malicious insiders for specific purposes by disclosing confidential information would seriously impact the competitiveness of the organization, and their dishonesty in information sharing would cause harm to various parties in the supply chain network because of disadvantage in information asymmetry.

2.3 Unintentional leakage

The term "unintentional" in this study implies "accidentally". Unintentional leakage occurs when an insider accidentally exposes critical business information not meant to be shared with third parties (Ritala et al., 2015; Tan et al., 2016). The accidental insider threat is the potential of an individual who has or had authorized access to an organization's network, system, or data through action or inaction, without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or value of the organization's information (Cappelli et al. 2012; Greitzer et al. 2014a; Greitzer et al., 2014b). Generally, the accidental insider which is inevitable in an organization is often the effect or symptom of deeper troubles (Bureau, 2013).

Most of the accidental insider threats, especially jobs which require protecting privileged information (sensitive, proprietary, or classified) pointed out human failures or errors could lead to an information breach or data loss (Liginlal et al., 2009 ; Greitzer et al., 2014). Errors could also occur in misperceptions and from a lack of awareness (Bureau, 2013). Such poor cognitive behavior is a method instigating undesirable behavior of unintentional leakage (Sonderegger, 2007). In normal circumstances, information is attended, comprehended, and aligned with the person's attitudes, beliefs, and motivations, after which decision-making processes produce behavioral responses (Bureau, 2013). However, the cognitive processes of perception, attention, comprehension, judgment/decision making could produce erroneous actions and behaviors (Bureau, 2013). In other words, poor cognitive process could have employees inadvertently or consciously make decisions to act inappropriately or unfavorably to their companies.

The unintentional information leakage could occur when employees are unclear about what they could actually disclose to business partners (Molok et al., 2010). Accidental insider threat correlates to poor situation awareness rather than to poor decision making, though decision making requires situation awareness (Endsley, 1995). Sometimes the over-enthusiasm about a new idea or innovative prospect could cause momentary negligence of protection responsibility when the other party is perceived as trustworthy (Greitzer et al., 2014a). To that end, professional pride could affect eagerness and willingness to share information, as could curiosity and passion (Fawcett et al, 2007). Incorrect or incomplete situation awareness at any given time may result in human error that causes unintentional leakage, potentially increasing organizational risk (Greitzer et al., 2014a).

The accidental insider has a history of causing information breaches as revealed in the examples above. The information unintentional leakage as an incident is merely a function of the insider's negligence. But egregious to a fault, accidental insider threat in disclosure of information can damage an organization's reputation and perhaps make it liable to pay damages to the injured party.

In sum, this section describes the human misbehaviors and perceptual weakness on intentional and unintentional leakages respectively. Intentional leakage is associated with malicious insider misbehavior while unintentional leakage is related to accidental insiders and their perception weakness. These are perennial problems showing an ever worsening and persistent research gap of which closure is elusive. These intentional and unintentional do not

seem to decrease and on the contrary, they increase from year to year (InfoWatch, 2016). The colossal financial losses attributed to both intentional and unintentional leakage deserve the attention of researchers especially when new and patches of technological defenses have failed (InfoWatch, 2016; Alneyadi et al., 2016). The next section will describe the research context, the data collection procedure and methodology. Noting the serious consequences and liabilities of human misbehaviour and weaknesses, the intentional and unintentional leakage, and the sparse research on human factors and leakage, this research is devoted to lay further groundwork to address leakages from the human perspective especially with the vulnerabilities at the human-computer interface.

3. Research Methodology

The infancy of information leakage on information sharing integrity research calls for an exploratory study (Saunders et al., 2009; Creswell, 2014). Qualitative research is primarily exploratory research. It provides the complex textual descriptions of how people experience the issue or problem under study (Mack yet al., 2005).

In order to have a better understanding of the concept of information leakage and how information leakage could impact information sharing integrity, it is necessary to look at the organization and its information exchange process. This study chooses to use case study approach because it aims at answering questions like "How" as well as the "Why", and to generate an in-depth, multi-faceted understanding of a complex phenomenon between information leakage and information sharing integrity in its real-life context (Yin, 2013). Besides, the use of case study approach can explore unknown variables in the phenomenon which is not fully understood yet (Voss et al., 2002) such as information leakage. Hence, the multiple-cases through holistic design of Yin (2013) is adopted to explore managerial approaches in mitigating the impact of intentional and unintentional leakage on information sharing integrity. The holistic cases in this study refer to the Malaysia Multinational Enterprise (MNE)/ Multinational Corporations (MNCs).

Section 3.1 describes the research context before section 3.2 justifies the case study approach and method; followed by section 3.3 which outlines the process of data collection.

3.1 Research Context

In Malaysia, the number of Multinational Enterprises (MNEs)/ Multinational Corporations (MNCs) has grown tremendously due to Malaysia's geographical location in the region, multilingual capabilities and abundance skill workers (Economic Transformation Programme, 2016). According to the World Investment Prospects Survey 2014-2016 FDI by the United Nations Conference on Trade and Development (UNCTAD), Malaysia ranks as among the world's top 15 attractive countries for foreign direct investment (FDI).

Malaysia is strategically located in the heart of South East Asia and offers a cost-competitive location for investor (MDBC, 2017). In this developing country with well-developed infrastructure, productive workforce, technological advancement, it also provides attractive incentives for investors (MIDA, 2017). As a result of perceptive foresight, Malaysia has a strong economic fundamental to attract foreign investors. The Star Online (2017) reported that Malaysia's 2017 full year gross domestic product (GDP) forecast to 5.3% which is higher than the GDP of 4.2% the year before. Factors that will drive economic growth for Malaysia include exports and private consumption (Ministry of Finance Malaysia, 2016). Moreover, Malaysian's inflation rate (CPI) was 2.1% is considered low and unemployment rate was 3.4% in 2016 (MIDA, 2017).

Furthermore, Malaysia has simple, transparent rules for registering a business, paying taxes earlier by introducing an online system for filling and paying goods and services tax (GST), getting credit to provide investors credit scores and registering property helps create a level playing field for doing business (The World Bank, 2017). According to its "Doing Business 2017" report, Malaysia is ranked 23 amongst 190 countries in the ease of doing business (The World Bank, 2017). Therefore, Malaysia is a business-friendly place that provides MNEs/MNCs with opportunities for growth and profits.

In recent years, leakages of confidential information in Multinational Enterprises (MNEs)/ Multinational Corporations (MNCs) have generated a great deal of discussion due to its severity which could harm the business environment (InfoWatch, 2016). The Global Data Leakage Report 2016 by InfoWatch presents the latest issue of information leakage in 2016. There were 1,556 leaks of confidential information reported and was worse than the same period the year before (InfoWatch, 2016). Among the data leaks logged, 38.2% of the cases were triggered by external attacks, while 61.8% were caused by internal offenders (InfoWatch, 2016). The Star Online (2016) reported that a total of 9,915 incidents were received by CyberSecurity Malaysia in 2015. Based on the current trend and scenario, this figure does not

include data breaches and records disclosed incidents that go unreported every day. All these incidents aimed at leaking confidential business information, disrupted critical operations, and jeopardised the Malaysian economy (The Star Online, 2016).

For the above reasons, much global attention is now focused on the need to mitigate information leakage in Multinational Enterprise (MNE)/ Multinational Corporation (MNC) of Malaysia. The Malaysia MNE/MNC therefore provides a rich and appropriate setting for exploring our research questions.

3.2 Multiple Case Study Approach

Multiple–case designs have increased in frequency in recent years (Yin, 2013). When exploring new areas, multiple-case study can augment external validity, guard against observer bias (Voss et al., 2002; Barratt et al., 2011), and the results obtained can improve generality (Voss et al., 2002; Yin, 2009). It also could create more robust and testable theories than those based on single case (Eisenhardt & Graebner, 2007; Yin, 2009).

The multiple-cases, holistic design is deemed appropriate because the selected cases are conceived as "replication logic" design (Yin, 2013). This replication logic used in multiple-case studies is similar to the multiple experiments (Yin, 2013). In this study, five cases of Malaysia Multinational Enterprise (MNE)/ Multinational Corporation (MNC) were examined. The selection of these companies was based on: (i) their MNEs/MNCs status, (ii) a physical presence (facilities and other assets) in the host country, and (iii) their practical understanding of the concept of information leakage. Each MNE/MNC case study must be carefully selected to predict similar results (literal replication) or predict contrasting results (theoretical replication) (Mills et al., 2010; Yin, 2013). In fact, the replications attempt to duplicate the exact MNE/MNC conditions of insider intentional leakage and unintentional leakage of confidential information to unauthorised parties and how MNE/MNC mitigate information leakage in order to achieve information sharing integrity. Therefore, overall evidences from multiple cases are sought regarding the information leakage impact upon information sharing integrity and are considered robust (Herriott & Firestone, 1983; Yin, 2009; Yin, 2013).

Before proceeding with data collection, all companies selected for this study must meet the following criteria: (i) companies are Multinational Enterprise (MNE) or Multinational

Corporation (MNC), (ii) companies have a physical presence in Malaysia, i.e. has facilities and other assets, and (iii) companies must well understand the concept of information leakage.

3.3 Data Collection

The companies which fulfilled all the above criteria were chosen from the Business Monitor International (BMI, 2017). The BMI provides online access to a large and rich database of Multinational Companies in emerging markets. The primary mode of data collection was interviewing; other methods employed included collecting printed documents.

In total, five semi-structured interviews were conducted to gather managerial approaches in mitigating the impact of information leakage in information sharing integrity. Semi-structured interviews can be very helpful in an exploratory study (Saunders et al., 2009). Besides, semi-structured interview is generally organised around a set of predetermined open-ended questions, with other questions emerging from the dialogue between interviewer and interviewee (DiCicco-Bloom & Crabtree, 2006). In this research, the interview questions were conducted on a one-to-one basis, between interviewee and interviewer, and took between 30 minutes to several hours to complete. All interviews were recorded and transcribed. By the end of the fifth interview, the incremental value added per interview was minimal and we were arguably approaching saturation.

In addition to the face-to-face interviews, the interviewer collected printed documents to supplement the information obtained from the five MNC/MNEs. These documents ranged from confidential documents (personal journals and diaries, letters, and e-mails) and public documents (company's brochure, catalogues, newspapers, and official reports) to other publicly available information (Creswell, 2014). The documents related to information sharing processes, policies and procedures of a company and performance improvements.

An overview of the companies and interviewees is provided in Table 1. The five MNC/MNEs are referred to as Company A, B, C, D and E. The data collection procedure is described in the following section.

3.3.1 Data Collection Procedure

The in-depth interviews were conducted in February 2017. In all five cases, appointments by email were made before visiting the companies. To ensure the interviewee has a clear understanding and could answer some questions, an introduction of research project together with the definition of information leakage and threats businesses face today were made. Besides, this offered the interviewee sufficient time to organize the relevant documents before interview session. A one-day site visit to each company was arranged with the duration of each semi-structured interview ranging from 45 minutes to 96 minutes with key interviewee. Finally, a chance to review documents related to information sharing processes, policies, company procedures and performance improvements before the end of the visit. During the interview, information was recorded by taking down notes and audiotaping. The interview protocol included the following:

1. Set the heading (date, place, interviewer, interviewee)
2. Prepare a short introduction for interviewee at the beginning, followed by questions and concluding statement.
3. When interviewee remains unduly silent, we explain their ideas in greater detail and discuss what they have said to help them express their ideas.
4. The lapses between the questions are meant to record responses
5. A final thank-you statement to acknowledge the time the interviewee spent during the interview.

The interview questions are provided in Appendix 1. Data and information collected from five cases are kept confidential at all times. To increase the truth-value of the study, one additional step was taken. The transcriptions and the summary of each interview were sent back to the respective interviewees for congruency with the information provided. The interviewees were given sufficient time to review and amend the contents. Any transcription discrepancy is resolved by seeking further advice from the relevant interviewee. This method was also used by Da Mota Pedrosa et al., (2012).

INSERT TABLE 1 ABOUT HERE

4. Data Analysis

With the aim of exploring managerial approaches in mitigating the impact of insider threat towards information leakage on information sharing integrity, the analysis thus involved codification of the interview transcripts to allow for qualitative analysis. All responses were imported into MAXQDA 12.0 software for coding, count and analysis.

During the analysis, a three-step qualitative data analysis was used (Miles & Huberman, 1994). First step involved the researcher reviewing the transcripts for accuracy and generating coding categories. The second step arranged codes similar category or theme into a cluster. In the final stage of the analysis, the findings were discussed, confirmed and reflected upon with key interviewees of the case companies where information leakage was studied.

To confirm the conclusion of the study and ensure validity, it is important to be aware of potential biases when analysing case study data. Most prominently is the potential that interviewees would play down their degree of information leakage throughout their companies in a positive light to protect their reputation. Generally, potential biases when analysing case study data do not appear in this study. This is because, when we explain information leakage to the interviewees, we portray leakage in a neutral state. For instance, we mentioned that information leakage is like know-how trading, is needed for technology transfer and the direction of its effect would depend on competition, exclusivity and instrumentality of the relationship (Schrader, 1989). As such, the interviewees were generally open about their shortcomings and potential biases were avoided.

4.1 Coding, calculation and analysis

The responses from the interviews were then imported into MAXQDA 12.0 software, a digital tool for qualitative analysis (Paulus, Lester & Dempster, 2014) to be coded, counted and analyzed.

4.1.1 MAXQDA's Code Matrix Browser

Figure 2 shows MAXQDA's Code Matrix Browser providing visualization of how often these five case companies' documents have been assigned specific codes. The matrix provides an overview of Company A, B, C, D, and E on x-axis, and specific codes (code system) on y-axis. The size of the symbol indicates how often the code has been used in a particular document of the company. The extreme right-hand column reports the number of segments of text codified for each code. The total number of coded segments assigned and retrieved is 112. The most frequently applied code is "Organizational Ethical Climate" with 36 segments codified. The second most frequent code appearing is "Information Security Culture" with 32 segments. These were followed by "Information Leakage" with 8 segments. Therefore, the analysis shows that the organizational ethical climate and information security culture are often seen as countermeasures for the information leakage.

INSERT FIGURE 2 ABOUT HERE

4.1.2 Conceptual Maps

MAXMaps tool combines analysis of study turning into conceptual maps. The last step of analysis in this study is to turn ideas and results into conceptual maps. MAXMaps tool is used for this, which has customized, standardized and pre-programmed visualizations (Paulus et al., 2014). The first is a standardized visualization for the category "Managerial Approaches." The second is a user-created conceptual model of "Information Leakage and Consequences." Figure 3 was created with the "Code-Subcode Model". The code of "organizational ethical climate" and "information security culture" were selected and the model automatically created. It shows the subcodes arranged around the selected code in the down and up coded segments. Each of the sub-codes is a managerial approach mentioned in the data set to mitigate the negative impacts of intentional leakage and unintentional leakage. All results were gathered into a conceptual map that brought together the causes (intentional leakage and

unintentional leakage), consequences and managerial approaches in mitigating the impact of information leakage.

INSERT FIGURE 3 ABOUT HERE

INSERT TABLE 2 ABOUT HERE

5. Discussions

From the interviews, Malaysia Multinational Enterprises/ Multinational Corporations (MNEs/MNCs) A, B, C, D and E revealed that information leakage occurred in their companies. We will now relate the findings to our research questions.

5.1 Why information leakage happens?

Earlier studies emphasize that information sharing has clear benefits but poses risk of information leakage that organizations must be aware of (Anand & Goyal, 2009; Lee & Whang, 2000; Li, 2002; Sharma & Routroy, 2016; Zhang et al., 2011; Zhang et al., 2012). In this study, we empirically identified the factors triggering information leakage and managerial approaches in mitigating negative consequences to achieve successful information integrity.

Our findings confirmed that leakage happens due to human factors. Human factors are the major challenge as company A, B, C, D, and E face information leakage either intentional or unintentional. Intentional leakage happened in the company due to personal greed other than organization benefit in which employees are willing to take risk over value of personal obsession, like what were mentioned by Company B and E. Besides, Company A employee's jealousy with others, disgruntled with company or feeling vindictive for any reasons also caused intentional leakage. Moreover, Company C and D faced malicious hackers who breached company's valuable information due to insufficient data protection Acts. Hence, all intentional human behaviors are unethical action to harm the security and business operations. These findings are consistent with past studies of insider threat (employees/malicious insider – associated with behavioural aspects of human) is the core factor that leads to information intentional leakage in an organization (Colwill, 2009; Mohamed et al., 2006; Warkentin & Willison, 2009).

In contrast, unintentional leakage happened due to negligent employees having breached their duty to protect, and accidentally leaking the valuable information to external parties, like what happened in Company B and C. Sometimes, employee's over-enthusiasm about a new idea and the company failed to educate employees about risky behaviors (like Company D) could also accidentally leaked information. In Company D, new employees' unintentional disclosure of valuable information due to employees being unclear about what they could actually disclose to partners. Thus, human error is a significant source that may damage or destroy information assets. These findings are also consistent with past studies of human error (employees/accidental insider – associated with lack of awareness) which revealed more information to authorized parties accidentally and is the core factor that leads to information unintentional leakage in an organization (Mohamed et al., 2006; Molok et al, 2010; Tan et al., 2016)

As such, the human factors that trigger information leakages can be summarized in Figure 4 below.

INSERT FIGURE 4 ABOUT HERE

5.2 How information leakage could impact information sharing integrity?

Every respondent (Company A-E) acknowledged that information leakage is critical because information of the company is lost or leaked to external parties either intentional or unintentional. The critical information disclosed may flow outside organizational borders in an uncontrollable, unwanted and harmful manner. This finding synchronizes with the findings from Ahmad et al., (2015) which shows the powerful impact of information leakage has devastating consequences on an organization. Any information shared or received that is unable to achieve real time transmission (in other words, leakage occurring in the transmission) will affect the overall efficiency and decapitate the process.

The interviewees proposed that information leakage causes one of the biggest threats to damage the companies. For example, Company A pointed out that disgruntled employees may intentionally leaked critical information to unauthorized parties. The unauthorized parties acknowledged the value of information to enhance their competency and mutually generate

new idea from the leaked information received. Similarly, Company B discovered the employee purposely breached confidential information to third parties for personal benefits. The threat of third parties could imitate a new innovation with little incentive to invest in R&D and innovation. It can be concluded that intentional leakage caused unauthorized parties gain as much innovation benefits, but companies involved have been awarded damages for loss of much higher quality information in the market. This is the two-edge sword of information intentional leakage, benefiting one end and risking the other end.

Although the growing significance of information sharing practices is good for organizations competitiveness and market performance, information leakage makes it difficult to achieve the goals and deliver a positive return on investment. Purchasing executive of Company D recounted that:

"The impact of information leakage is unexpected and out of control in the company. Our company was over-enthusiastic about a new idea to achieve its mission, values and goals but failed to educate employees about risky behaviours that could unintentionally leak data and information. Therefore, our company had to invest huge resources developing security policies in order to mitigate information leakage. This is the only way to achieve its goals and deliver higher return".

In the meanwhile, Company E admitted that information leakage led to lack of trust with partners. Hence, partners are unwilling to share information due to disclosure of any confidential information without partner's consent. Therefore, information sharing collaboration is difficult to accomplish and facilitate information sharing for maximum efficiency and effectiveness.

"Our company faced up supplier's information was leaked to third parties. The trust among suppliers was broken and the reputation is ruined' - Project program analyst of Company E

Moreover, Company D revealed that information leakage is a risk undermining the effectiveness of information sharing. Through the information sharing process, information sent or received should not be manifested or else accuracy and mutual expectation on information would not be achieved as the information shared can be considered useless in an organization. In other words, the loss of usefulness or value of the leaked information damages the integrity of information sharing.

As such, with the above negative outcomes, intentional leakage and unintentional leakage would cause information sharing disruption in an organization. In other words, leakage negatively affects information sharing integrity and this was concluded by the firms in this study. Firms that encounter higher frequency of leakages will cause negative impact to their information sharing integrity. Hence, appropriate measures are required to mitigate the effects of information leakages on information sharing integrity.

5.3 How information leakage can be mitigated?

The analysis of the results showed that there were several approaches/strategies to risk (information leakage) reduction measures reported by the case companies. These mitigation strategies are human governance measures that could be categorized as fostering organizational ethical climate and information security culture. Human governance refers to human beings guided by a common set of principles inherent in every human being; these unwritten principles are built into each and every human irrespective of colour or creed, to help human differentiate between right and wrong and how to treat each fellow human being (Salleh, 2016).

Human governance encompasses ethics and culture because through its practice, it acts as a moral compass which can eventually bring out integrity which is a symbol of inner state of values. Human internal character needs to be nurtured in order to encourage integrity. Organizational ethical climate (OEC) reflects the shared perceptions held by employees regarding the organization's norms, policies, practices and procedures (Nedkovski, Guerci, De Battisti, & Siletti, 2017). Organizational ethical climate facilitates ethical behaviour in organizations in response to ethical dilemma especially caused by employees. On the other hand, information security culture reflects the way of doing things around the information security, including creation of an environment that fosters and nurtures shared security basic assumption, attitudes and beliefs, value and knowledge in a given organization (Schlienger & Teufel, 2002; Da Veiga & Martins, 2015). Information security culture shapes employee's attitude and behaviours towards information security in the long run (Chen et al., 2015).

a) Organizational Ethical Climate (OEC)

The case companies relied on organizational ethical climate as shared perception on what correct behavior is and how ethical situations should be handled in an organization. This

synchronizes with the notion of OEC in literature of Victor & Cullen (1987, 1988). Ethical climate influences both the decision-making and subsequent behaviour in response to ethical dilemmas (Hsieh & Wang, 2016; Martin & Cullen, 2006; Simha & Cullen, 2012). Victor et al. (1988) highlighted that there are five types of ethical climate that exist in companies in order to mitigate employees deliberate disclosure of confidential information to unauthorized parties. Our findings reveal that the facilitation of ethical behavior in each case company differs from one another. The reason is the companies have different locus analysis of ethical climate. As such, in the following section, we discuss the mapping of our interview findings with the ethical climate-locus of analysis. For clarity, the types of ethical climate and the division of the analysis locus will be based on Victor et al. (1988) as shown in Figure 5.

INSERT FIGURE 5 ABOUT HERE

Instrumental

Leakage of critical information usually occurs through employee personal greed rather bringing benefits to the organization. To prevent unethical employees breaching confidential information intentionally in a company, instrumental ethical climate might be legitimized by the self-interest behavior prevalent in workplace. Likewise, the decision has been made that takes everyone's interests into account to serve the company's interests. Employee's prime purpose is to ultimately serve their self-interest, also it is his sense of obligation to others. For example, Companies E offer progressive reward systems which motivated employees to work at higher levels of productivity in order to be more effective to achieve its goals in long term future.

Caring

Employee's jealousy of others or feeling vindictive for any reasons also caused intentional leakage in an organization. In the high-profile data breaches that frequently damages a company's reputation and profits, caring ethical climate is one of the most desired climate by employees. Individuals perceive that decisions should be based on an overarching concern for the well-being of others in organization. The general manager of Company A suggested that creation of a great working environment that makes employees feel a part of it can mitigate

employee's jealousy or feeling vindictive of others. Therefore, employees are willing to put much time and energy into the job and hard work generates loyalty. For these reasons human behavioral cause for intentional leakage can be reduced.

Independence

The employee is guided by their own personal ethics in an organization. The most important concern is each person's perception of information leakage is unique and different from one another. The general manager of company A explained that many of the employees believe that even though they had intentionally leak information for personal gain, they can still get away from disciplinary action. To mitigate the leakage of information in workplace, employees must have high personal moral value with minimal regard for external forces or outside influence on ethical quandaries. Independence ethical climate sometimes is suitable in this case (e.g., for company A). The decisions are made based on careful consideration by the employees themselves on what is right and wrong behavior before they executed their actions.

Rules

The analysis of the results from the Company A, C and D saw strict policies and procedures in place that prohibit employees from communicating critical information to unauthorized parties. In the rules ethics climate, organizational decisions are perceived as being guided by a strong and pervasive set of policies and procedures. Employees follow operating practices under strict organization policies and procedures. The chances are likely that these rules will be followed by everyone in the organization. The rules ensured all employees are doing the right thing to prevent outrageous workplace behaviour. These policies and procedures are to assist employees in understanding the difference between "Right" and "Wrong" to prevent unethical behaviour. Respondents emphasised that to reduce the risk of intentional leakage, employees act in an ethical manner guided by the organisational policies and procedures.

Law and Code

The continued effort to strengthen law and ethical code climates, the case companies are responsible for interpreting confidentiality restrictions imposed by laws and statutes to all levels of employee. For example, human resource officer from Company C revealed that they implemented "Criminal Code" to prevent employees or former employees from leaking confidential information to unauthorized parties. Besides, the company has a comprehensive code of conduct which can provide extra protection for information assets and can serve to keep out legal trouble. Hence, employees are expected to strictly follow legal or professional standards especially decision maker who must take into account all relevant considerations before action.

b) Information Security Culture

Our findings also reveal another important mitigation approach i.e. information security culture. Participants in this research reported that information breaches are often caused by employees' negligence or ignorance of information sharing, resulting in large financial losses for organizations. The case companies asserted that information security culture will minimize unintentional leakage. This finding echoes the same tune as Al Hogail & ALHogail (2015). Through information security culture, appropriate information security beliefs and values that guide employee behaviour will be constructed when interacting with information assets and information technology systems. Hence, this helps minimize unintentional leakage.

Several of the case companies stated that information security policies and procedures are to protect the confidentiality, integrity and availability of the information assets. For instance, Company A developed an information classification to limit access information and facilitate more efficient information exchange activities. Information classification would classify information into three confidential levels (confidential, restricted and internal use) and public level. Based on the information confidential levels, employees have comprehensive good practice guidance about the appropriate information that can be shared.

Another example of information security culture is the setting up of an information access policy, which is allowing only limited number of persons to access such information in the company. Company C creates and enforces a strict access policy could easily monitor the activities of these employees and make use of information effectively. For example, User Activity Monitoring was used by Company C to deter user access to the files and track in detail any privileged user activity. An automated screen locks down after unauthorized user accessed

the network. This system appears to be useful to tackle network vulnerability that enhance processing, transmission and storage information to authorized users.

Moreover, Company D also recommended enforcement of strong password policy to enhance safeguard of company devices. The company creates and enforces strong password policy to enhance its computer security. Passwords provide strong protection against employees who are not as knowledgeable about proper business information security precautions. The respondent from Company D further reiterated that in fact, secret passwords have always been used for validating user identity. Therefore, Company D emphasizes password setting on specific document as a safeguard device to prevent information leakage.

In addition, fostering information security culture through sufficient training and proper education are also important to inoculate such security consciousness at all levels of employees. The case companies mentioned that it is important to understand the types of risk behaviours associated and make it as simple as possible through education, training and awareness programs. Besides, companies must ensure employees participation in relevant programs to keep abreast with information security. It is good enough to provide a security checklist to guide employees follow policies and procedures. All these programs assist organizations in creating and sustaining a security conscious culture to mitigate unintentional leakage.

In sum, clear expectations of appropriate behaviours of employees need to be thoroughly embedded in information security control. Information security culture increased awareness of unintentional leakage issues and reinforces an implicit adherence to security conduct.

6. Managerial Implications and Proposed Framework

The findings from this study give valuable managerial implications. Firstly, the findings imply that managers of companies must be aware of the key factors of human misbehaviour and perceptual weaknesses could trigger information leakage. The human factor plays a very important role in information sharing, especially, when companies have weak internal controls. By engaging in information sharing, companies increase the risk that confidential information might be intentionally or unintentionally leaked to unauthorized parties. Risks from human activities are dangerous to information assets, especially from those who are within the organization i.e. the insiders. This is because insiders will know how, when and where to attack and how to cover their tracks. Intentional leakage is caused by malicious insiders with

intentional behavior to leak information. Unintentional leakage is caused by accidental insiders who do not have intention to leak information but have acted inappropriately due to perceptual errors.

The second implication is managers of companies need to be aware of the harmful effects of information leakage that can seriously affect information sharing integrity. The critical information disclosed may flow outside organizational borders in an uncontrolled manner resulting in loss of information value. Thus, intentional and unintentional leakages by insiders would disrupt information sharing in an organization. It is imperative for managers to be cognizant and mindful of insiders threat. Hence, to overcome information leakage by insiders, mitigation on human factors need to be undertaken by managers. Human factors should be examined in the context of governance (hard and soft measures) in information sharing.

Interestingly, our findings imply managers and practitioners should foster organizational ethical climate and information security culture because they are useful to promote diffusion of central norms and values which can lead to an increased collective awareness of leakage issues. This corresponds to the hard and soft measures of human governance. Foremost, companies can benefit by establishing this coherent human governance structure i.e. ethical climate and information security culture, as these indirectly contribute to information sharing integrity by means of mitigating intentional and unintentional leakages.

These governance measures are imperative for managers and practitioners to combat leakage issues. To address intentional leakage, we advocate managers to foster organizational ethical climate to shape and guide employees' acceptable behaviour. This is because only through these collective ethical norms, employees' purposeful disclosure of sensitive information can be countered. For example, managers can create a great working environment (caring ethics), offer progressive reward system (instrumental ethics), have strict policies and procedures (rules ethics) and implement criminal code (law and code ethics) to foster conducive organizational ethical climate to nurture employees' behaviour. On the other hand, we advocate managers to implement an information security culture e.g. setup information access and password policies to safeguard information assets from accidental loss through unexpected system failure or human error. Companies can also organize frequent training and education to instil information security conscious in all levels of employees.

Noting the above, societies at large could benefit from employees who would inculcate or spill over good organizational ethical culture to influence their private homes. Good ethical influences in homes could multiply to schools by school going children or to workplaces by family members who work in other organizations. Slowly but surely, a pervasive ethical climate would gain a foothold in daily lives making ethical behaviour second nature. Good ethics should promote a society which is clean from corruption.

Even information security culture could rub onto family members who would also bring this culture to their workplace. The conscious decision to maintain an information secure work environment augurs well for personal data protection similar to the hard measure of personal safety protection.

The suggestions by the five companies to introduce organization ethical culture and information security culture reflect the advocacy in literature. Therefore, this research has bridged research and practice. The value-added impact of these advocacies is the multiplier effect of trust and commerce. When commerce is surrounded by mutual trust, it is expected business would flourish with lower transaction costs.

Finally, this study proposed an exploratory framework that characterizes the significant relationships between information leakage and information sharing integrity.

INSERT FIGURE 6 ABOUT HERE

Figure 6 presents a framework that characterizes information leakage, the devastating consequences on information sharing integrity, and the human governance measures that help mitigate the iniquities of humans in sharing information. This framework could be a guide for practitioners to overcome information leakage issue in information sharing. The framework could also be further evaluated using empirical studies in future research to investigate the correlation that exists between human governance measures and information leakage.

7. Conclusion

This study adds value to the existing research and literature by highlighting the importance of human governance through fostering organizational ethical climate and information security culture in mitigating information leakage to achieve information sharing

integrity, especially when companies have weak internal controls in information sharing. Practically, this study contributes to the industry and business that are striving towards solving the mounting problem of information leakage. Theoretically, this study adds value to the existing literature by raising the human factors such as the behavioural perspective of malicious insiders and cognitive perspective of accidental insiders, links to appropriate mitigation or governance strategies to pre-empt information leakage. Human factors and human governance deserve more research attention so managers and practitioners could take appropriate strategies to avert information leakage in order to achieve efficient and effective information sharing. This paper also contributes a research framework which could be a guide to overcome information leakage issue in information sharing.

This research is not without limitations. The current study involved MNC/MNEs operating in Malaysia while companies in other countries may have different ethical climate and information sharing culture. Thus, for future research, it will be good to replicate the study in a larger geographic region to verify the findings and insights of this research. We also highly recommend that inter-organizational information sharing of the case MNEs/MNCs should be solicited for further details when extending this study in the near future. This would allow the researcher to discover new insights into mitigating the impact of information leakage among the two parties in information sharing collaboration especially in supply chain integration. Besides, the applicability of a large-scale survey to verify the exploratory insights of this research and triangulate (two or more methods) its findings are suggested. Future research could possibly investigate the correlation between intentional leakage and unintentional leakage that can be addressed by organizational ethical climate (OEC) and information sharing culture (ISC) separately in order to achieve information sharing integrity.

Acknowledgments

The authors would like to thank the Academy of Sciences Malaysia, British Academy and Newton-Ungku Omar Fund [grant number 304 / PMGT / 650912 / B130] and Fundamental Research Grant Scheme [203/PMGT/6711513] to complete this research project.

References

Ahmad, A., Tscherning, H., Bosua, R., & Scheepers, R. (2015). Guarding against the erosion of competitive advantage: A knowledge leakage mitigation model. *Computers & Security, 42,* 27-49.

Alneyadi, S., Elankayer, S., and Vallipuram, M. 2016. "A survey on data leakage prevention systems," *Journal of Network and Computer Applications* (62), pp. 137-152.

Al Hogail, A., & AlHogail, A. (2015). Cultivating and assessing an organizational information security culture: An empirical study. *International Journal of Security and Its Applications*, *9*(7), 163-178.

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. In *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on* (pp. 1-7). IEEE.

American Psychological Association (2017). Glossary of psychological terms. Retrieved September 18, 2017, from http://www.apa.org/research/action/glossary.aspx?tab=2

Anand, K. S., & Goyal, M. (2009). Strategic information management under leakage in a supply chain. *Management Science*, *55*(3), 438-452.

Barratt, M., Choi, T. Y., & Li, M. (2011). Qualitative case studies in operations management: Trends, research outcomes, and future research implications. *Journal of Operations Management*, *29*(4), 329-342.

Bureau, F. I. P. (2013). Unintentional Insider Threats: A Foundational Study. Retrived from August, 28, 2017, from http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

Business Monitor International (2016). Multinational Companies in Malaysia Online Database. BMIResearch – A FitchGroup Company.

Cannella, S., Framinan, J. M., Bruccoleri, M., Barbosa-Póvoa, A. P., & Relvas, S. (2015). The effect of inventory record inaccuracy in information exchange supply chains. *European Journal of Operational Research*, *243*(1), 120-129.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Upper Saddle River, NJ: Pearson Education, Inc.

Cappelli, D. M., Moore, A. P., Trzeciak, R. F., & Shimeall, T. J. (2009). Common sense guide to prevention and detection of insider threat. *CERT Insider Threat Study Team, Carnegie Mellon University*. Retrieved from https://pdfs.semanticscholar.org/0a54/b1b543b32e8ce57887c149c2bf92d986b1c2.pdf

Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.

Cheng, L.; Li, Y.; Li, W.; Holm, E.; and Zhai, Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers and Security, 39 (2013), 447–459.

Colwill, C. (2009). Human factors in information security: The insider threat–who can you trust these days? *Information security technical report*, *14*(4), 186-196.

Crossler, R.E.; Johnston, A.C.; Lowry, P.B.; Hu, Q.; Warkentin, M.; and Baskerville, R. Future directions for behavioral information security research. *Computers and Security*, 32 (2013), 90–101.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, California: SAGE Publications, Inc.

Creswell, J. W., & Inquiry, Q. (2007). *Research Design: Choosing among five approaches*. London, UK: SAGE Publications, Inc.

Da Mota Pedrosa, A., Näslund, D., & Jasmand, C. (2012). Logistics case study based research: Towards higher quality. *International Journal of Physical Distribution & Logistics Management*, *42*(3), 275-295.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*. *49*, 162-176.

Dai, H., Li, J., Yan, N., & Zhou, W. (2016). Bullwhip effect and supply chain costs with low- and high-quality information on inventory shrinkage. *European Journal of Operational Research*, *250*(2), 457-469.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, *40*(4), 314-321.

Dimotakis, N., Ilies, R., & Mount, M. K. (2008). Intentional negative behaviors at work. In *Research in Personnel and Human Resources Management* (pp. 247-277). Emerald Group Publishing Limited.

Durugbo, C., Tiwari, A., & R. Alcock, J. (2014). Managing integrated information flow for delivery reliability. *Industrial Management & Data Systems*, *114*(4), 628-651.

Economic Transformation Programme (2016). More MNCs keen to take advantage of country's location. Retrieved August 10, 2017, from http://etp.pemandu.gov.my/Related_Stories-@ More_MNCs_keen_to_take_advantage_of_countrys_location.aspx

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25-32.

Endsley, M. R. (1995). A taxonomy of situation awareness errors. *Human Factors in Aviation Operations*, *3*(2), 287-292.

Fawcett, S. E., Osterhaus, P., Magnan, G. M., Brau, J. C., & McCarter, M. W. (2007). Information sharing and supply chain performance: The role of connectivity and willingness. *Supply Chain Management: An International Journal*, *12*(5), 358-368.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. *Insider Threats in Cyber Security*, 85-113.

Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, *4*(2), 25.

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security & Privacy*, *6*(1), 61-64.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014a). Analysis of unintentional insider threats deriving from social engineering exploits. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 236-250). IEEE.

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014b). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 2025-2034). IEEE.

Gruys, M. L., & Sackett, P. R. (2003). Investigating the dimensionality of counterproductive work behavior. *International Journal of Selection and Assessment*, *11*(1), 30-42.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Haines, R., and Leonard, L.N.K. Individual characteristics and ethical decision-making in an IT context. Industrial Management and Data Systems, 107, 1 (2007), 5–20.

Harhoff, D., Henkel, J., Hippel, E. (2003). Profiting from voluntary information spillovers: how users benefit by freely revealing their innovations. *Research Policy*, 32, 1753-1769.

Hatala, J. P., & George Lutta, J. (2009). Managing information sharing within an organizational setting: A social network perspective. *Performance Improvement Quarterly*, *21*(4), 5-33.

Herriott, R. E., & Firestone, W. A. (1983). Multisite qualitative policy research: Optimizing description and generalizability. *Educational Researcher*, *12*(2), 14-19.

Hoecht, A., & Trott, P. (2006). Outsourcing, information leakage and the risk of losing technology-based competencies. *European Business Review*, *18*(5), 395-412.

Hsieh, H. H., & Wang, Y. D. (2016). Linking perceived ethical climate to organizational deviance: The cognitive, affective, and attitudinal mechanisms. *Journal of Business Research*, *69*(9), 3600-3608.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats: An overview of definitions and mitigation techniques. *JoWUA*, *2*(1), 4-27.

Huong Tran, T. T., Childerhouse, P., & Deakins, E. (2016). Supply chain information sharing: Challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management*, *27*(8), 1102-1126.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers*, *15*(1), 1-4.

InfoWatch, 2016. *Global data leakage report, 2016.* Retrieved August 10, 2017, from https://infowatch.com/node/2654/done?sid=3412

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, *42*(6), 983-991.

Kajzer, M.; D'Arcy, J.; Crowell, C.R.; Striegel, A.; and Van Bruggen, D. An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, 43 (2014), 64–76.

Kembro, J., Näslund, D., & Olhager, J. (2017). Information sharing across multiple supply chain tiers: A Delphi study on antecedents. *International Journal of Production Economics*, *193*, 77-86.

Kwak, J. K., & Gavirneni, S. (2015). Impact of information errors on supply chain performance. *Journal of the Operational Research Society*, *66*(2), 288-298.

Kwon, I. W. G., & Suh, T. (2005). Trust, commitment and relationships in supply chain management: A path analysis. *Supply Chain Management: An International Journal*, *10*(1), 26-33.

Lee, H. L., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Manufacturing Technology and Management*, *1*(1), 79-93.

Li, L. (2002). Information sharing in a supply chain with horizontal competition. *Management Science*, *48*(9), 1196-1212.

Liang, H., and Xue, Y. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11, 7 (2010), 394–413.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers and Security*, *28*(3), 215-228.

Mack, N., Woodsong, C., MacQueen, K. M., Guest, G., & Namey, E. (2005). *Qualitative research methods: A data collectors field guide*. Durham, NC: Family Health International

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers and Security*, *24*(5), 371-380.

Malaysian Dutch Business Council (MDBC). 2017. Malaysia. Retrieved from August 3, 2017, from http://www.mdbc.com.my/information/country-information/malaysia/

Malaysian Investment Development Authority (MIDA). (2017). Why Malaysia? Retrieved August 4, 2017, from http://www.mida.gov.my/home/why-malaysia/posts/

Marcus, B., Anita Taylor, O., Hastings, S. E., Sturm, A., & Weigelt, O. (2016). The Structure of Counterproductive Work Behavior: A Review, a Structural Meta-Analysis, and a Primary Study. *Journal of Management*, 42(1), 203–233. https://doi.org/10.1177/0149206313503019

Martin, K. D., & Cullen, J. B. (2006). Continuities and extensions of ethical climate theory: A meta-analytic review. *Journal of Business Ethics*, *69*(2), 175-194.

McCormick, M. (2008). Data theft: A prototypical insider threat. *Insider Attack and Cyber Security*, *39*, 53-68.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Beverly Hills, CA: SAGE Publications, Inc.

Mills, A. J., Durepos, G., & Wiebe, E. (2010). *Multiple-case designs: Encyclopedia of case Study Research.* London, UK: SAGE Publications, Ltd. Retrieved from http://methods.sagepub.com/reference/encyc-of-case-study-research/n216.xml

Ministry of Finance Malaysia. (2016). 2017 Economic report. Retrieved August 10, 2017, from http://www.treasury.gov.my/index.php/en/economy/economic-report.html

Mohamed, S., Mynors, D., Grantham, A., Walsh, K., & Chan, P. (2006). Understanding one aspect of the knowledge leakage concept: People. In *Proceedings of the European and Mediterranean Conference on Information Systems (EMCIS),* July 6th-7th 2006, Alicante, Spain, (2006).

Molok, N. N. A., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. *ACIS 2010 Proceedings.* Retrieved from http://works.bepress.com/nurul_abdulmolok/1/

Moore, A., Cappelli, D., Caron, T., Shaw, E., & Trzeciak, R. (2009). Insider theft of intellectual property for business advantage: A preliminary model. *CEUR Workshop Preceedings, 1*(469), 1-21.

Nayar, M. K. (2004). Information integrity (I* I): The next quality frontier. *Total Quality Management & Business Excellence*, *15*(5-6), 743-751.

Nedkovski, V., Guerci, M., De Battisti, F., & Siletti, E. (2017). Organizational ethical climates and employee's trust in colleagues, the supervisor, and the organization. *Journal of Business Research*, *71*, 19-26.

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: An assessment and mitigation framework. *Journal of Enterprise Information Management*, *20*(6), 677-699.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014, May). Understanding insider threat: A framework for characterising attacks. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 214-228). IEEE.

Okere, I., Van Niekerk, J., & Carroll, M. (2012). Assessing information security culture: A critical analysis of current approaches. In *Information Security for South Africa (ISSA), 2012*(pp. 1-8). IEEE.

Olzak T.Data leakage: Catching water in a sieve [Blogpost]. Retrieved from ⟨http://blogs.csoonline.com/1187/DataLeakage⟩; 2010.

Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 162-172). IGI Global.

Orgill G L, Bailey MG, & Orgill P M. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Paper presented at the Proceedings of the 5th conference on Information technology education. Salt Lake City, UT, USA; 2004. p.177–81.

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems*, *92*, 47-56.

Paulus, T., Lester, J., & Dempster, P. (2014). *Digital tools for qualitative research*. London, UK: SAGE Publications, Ltd.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security*, *28*(8), 816-826.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, *35*, 22-31.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal*, *38*(2), 555-572.

Sackett, P. R., & DeVore, C. J. (2001). Counterproductive behaviors at work. *Handbook of Industrial, Work, and Organizational Psychology*, *1*, 145-164.

Salleh, A. (2016). Human Governance: Bringing the Meaning of Integrity in the Life of Professional Accountants. Working paper, Putra Graduate School of Business.

Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students.* Harlow, England: Pearson Education Limited.

Schlienger, T., & Teufel, S. (2002). Information security culture. *In Security in the Information Society* (pp. 191-201). Salmon Tower Building, New York City: Springer US.

Sharma, S., & Routroy, S. (2016). Modeling information risk in supply chain using Bayesian networks. *Journal of Enterprise Information Management*, *29*(2), 238-254.

Schrader, S. (1989). Informal Technology Transfer between companies: Information Leakage or Know-how Trading?. Working paper WP# 3007-89-BPS, Sloan School of Management, MIT, Cambridge.

Simha, A., & Cullen, J. B. (2012). Ethical climates and their effects on organizational outcomes: Implications from the past and prophecies for the future. *The Academy of Management Perspectives*, *26*(4), 20-34.

Sonderegger, T. (2007). *Cliffs Quick Review: Psychology*. NY, NY: Wiley Publishing, Inc.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124-133.

Stoneburner, G., Goguen, A., Feringa, A. (2002) Risk management guide for information technology systems, National Institute of Standards and Technology SP800-3. U.S. Government Printing Office. Retrieved form http://csrc.nist.gov/publications/nistpubs/800–30/ sp800–30.pdf (2002)

Sumner, J., Cantiello, J., Cortelyou-Ward, K., & Noblin, A. M. (2012). Information sharing among health care employers: Using technology to create an advantageous culture of sharing. In *Annual Review of Health Care Management: Strategy and Policy Perspectives on Reforming Health Systems* (pp. 123-141). Emerald Group Publishing Limited.

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and knowledge leakage in supply chain. *Information Systems Frontiers*, *18*(3), 621-638.

The Star Online (2016). Facing cyberattacks in 2016 and beyond. Retrieved Jan 1, 2017, from https://www.thestar.com.my/tech/tech-opinion/2016/01/28/facing-cyber-attacks-in-2016-and-beyond/

The Star Online (2017). Stronger economic growth for 2017. Retrieved August 10, 2017, from http://www.thestar.com.my/business/business-news/2017/07/04/stronger-economic-growth-for-2017/

The World Bank Group (2017). Doing business 2017: Equal opportunity for all. Retrieved August 10, 2017, from http://www.doingbusiness.org/reports/global-reports/doing-business-2017

Tseng, F. C., & Fan, Y. J. (2011). Exploring the influence of organizational ethical climate on knowledge management. *Journal of Business Ethics,101*(2), 325-342.

United Nations Conference on Trade and Development. (2016). World investment prospects survey 2014-2016. Retrieved August 10, 2017, from http://unctad.org/en/pages/publications/World-Investment-Prospects-Survey.aspx

Victor, B., & Cullen, J. B. (1987). A theory and measure of ethical climate in organizations. *Research in Corporate Social Performance and Policy*, *9*(1), 51-71.

Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. *Administrative Science Quarterly, 33*, 101-125.

Voss, C., Tsikriktsis, N., & Frohlich, M. (2002). Case research in operations management. *International Journal of Operations and Production Management*, *22*(2), 195-219.

Warkentin, M., & Willison, R. (2009). Behavioural and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101.

Willison, R., and Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37, 1 (2013), 1–20.

Yin, R. K. (2009). *Case study research: Design and methods*. London, UK: SAGE Publications Ltd.

Yin, R. K. (2013). *Case study research: Design and methods*. London, UK: SAGE Publications Ltd.

Zhang, D. Y., Cao, X., Wang, L., & Zeng, Y. (2012). Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection. *Journal of Intelligent Manufacturing*, *23*(4), 1351-1364.

Zhang, D. Y., Zeng, Y., Wang, L., Li, H., & Geng, Y. (2011). Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry*, *62*(3), 351-363.

APPENDIX 1 : Interview Questions

Q01	What are your views about information sharing? Its benefits and perils.
Q02	With regards to information leakages, were there any such occurrences in your company?
Q03	Did your company identify the perpetrator? Was the perpetrator a man or woman? Was he/she an executive, manager or a senior manager?
Q04	What motivated the perpetrator to leak company data and information? What information was leaked then?
Q05	How was the leakage dealt with by your company?
Q06	In your opinion, how could a company prevent information leakage?
Q07	Does your company have a code of ethics and what is the code about? How is this code communicated to employees? How does the company deal with employees breaking such codes?
Q08	Has the code of ethics in anyway helped prevent or reduce information leakages? Has this code of ethics stopped you from leaking information?
Q09	Why are such codes of ethics unable to stop information leakages?
Q10	What do you fear most to deter you from committing an unauthorized information leak? Do you think your colleagues share this view?
Q11	Let us discuss information security culture or habits. Are you always mindful of information protection and leakages?
Q12	How frequent does your company remind you to safeguard data and information? How does the company communicate these reminders?
Q13	We just want to find out the reality of things. Do you really care about these reminders? Why?
Q14	Do you and your friends or colleagues talk about work (suppliers, contractors, and customers) during tea time and lunch hour?
Q15	What would stop you from talking about work during tea time and lunch hour?
Q16	Do you think it is possible to prevent information leakage? How and why? But is it practical?
Q17	Does your company educate you about risky behaviours that could unintentionally leak data and information? In spite of such education, employees continue to show risky behaviours and put data at risks. Why is this so? What could change these risk behaviours?
Q18	Who do you think are most likely to leak data and information? Could you profile perpetrators? Why? Have you encountered repeat offenders?
Q19	What types of information are usually leaked? Could they be controlled?
Q20	How does your company respond to a leakage? Keep quiet about it. Officially announce in the company bulletin board. “Leaked” such occurrences/incidences to employees through the grapevine. Hinting to employees. What do you think your company was trying to achieve?
Q21	Do you think a company could stop a perpetrator before the information leakage occurs?

Q22	Do you think it is good and effective to give rewards to informers or "whistle blowers" or recipients of such information before the perpetrator intentionally leaks information? Why?
Q23	Do you think data and information would be safer in the future?
Q24	How does your company foster the development of highly ethical, accountable and professional behaviour?
Q25	Would a more stringent data protection act be helpful to curb information leakage?
Q26	Do you think companies could criminalize (to declare illegal or to outlaw) information leakage (intentional and unintentional) just like the Official Secrets Act? Is it practical?
Q27	Are there ways to detect an imminent data and information leakage?
Q28	One of the greatest irony is "we do not know when data or information is lost." If this is true, how do we then know when and to whom data and information is lost?