CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

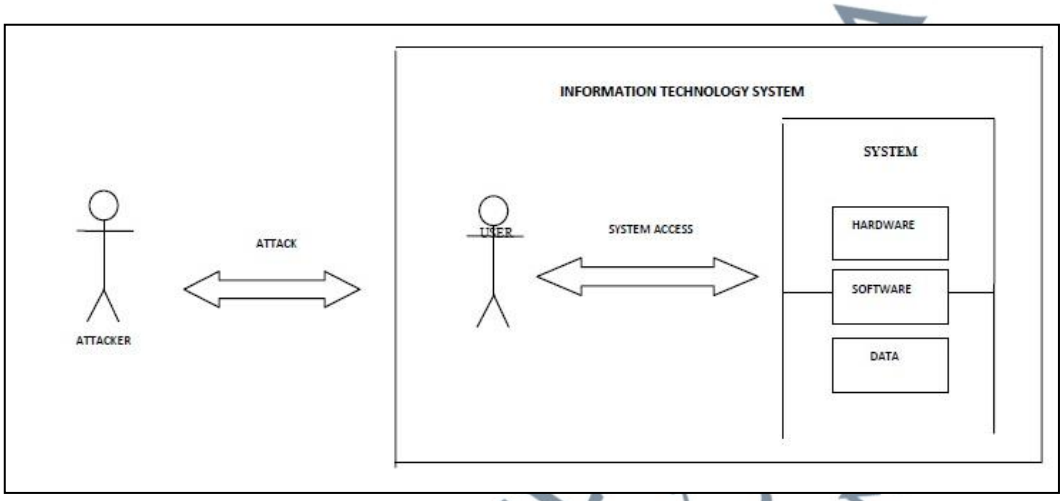
This chapter examines and reviews the existing literature related to unintentional insider threats. In particular, this chapter examines the problem of unintentional insider threat (UIT) by providing an operational definition of UIT, reviewing relevant research to gain a better understanding of its causes and contributing factors, providing examples of UIT cases and the frequencies of UIT occurrences , the UIT in Malaysia and presenting the potential mitigation strategies and countermeasures and its limitations.

2.2. Role of Human in Information Security

The goal of system security is ensuring data confidentiality, integrity and availability (Pfleeger, 2003; Bishop, 2003). A threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either intentional example hacking or accidental, for example the possibility of a computer malfunctioning, or the possibility of a natural disaster (Yadav & Shashant, 2014). The major security threats in information system are four key types which are human unintentional threats, human intentional threats, technological threats and environmental threats (Jouini et al, 2014; Malami et al., 2012).

Information Security is not just a technology issue; rather, it is affected to a high extent by people. Organizations depend on people, their behaviour and ethics, and their awareness (Morrill, 2007).

Though risks are involved in every aspect of Information Security, industry experts generally believe that the weakest link is the humans (Albrechtsen, 2007). The elements of information technology system that are at risk of attacks are presented in Figure 2.1.



Source: Nikolakopoulos (2009)

Figure 2. 1: Linking the Human Factor

It is true that all employees do not try to cause damage intentionally. For instance, in a certain incident, an employee sent confidential company information to a newspaper by mistake. In another case, the Norwegian National Security Authority found trade secrets and security information in the Facebook profiles of a few of their employees (Albrechtsen, 2007).

These examples show the poor behaviour of users or their lack of awareness. Various such scenarios were determined by Mitnick and Simon (2002), in which employees are tricked into security violations, for example the use of social engineering and phishing attacks to infiltrate information systems and manipulate people to carry out their desired actions.

A serious threat is posed by employees by presenting different vulnerabilities, regardless of whether they are ignorant, negligent, have been tricked or are acting

intentionally. Therefore, adequate mechanisms should be enforced to avoid information security violations by all the employees. These methods should include physical as well as functional aspects and should not be entirely dependent on technology as that would lead to ineffective outcomes (Sklet, 2006).

Individuals will make behaviour al decisions on the basis of their estimates of the risks related to the different alternatives. Optimism bias as well as cumulative risk has an impact on these decisions. Optimism bias means that majority of the people are not aware of the fact that they are at risk. Rather, these people are of the view that others have greater probability of experiencing negative outcomes (Parsons et al., 2010). It is typically believed by most users that hackers would not give importance to the information on their computers, which is why users are unlikely to consider them as possible targets (McIlwraith, 2006). The optimism bias can cause the security-related risks to increase because the risk may be underestimated by the individuals and hence, may not stay updated with security patches and adhere to other security protocols (Parsons et al., 2010). People will essentially underestimate the possibility of their actions or inactions leading to a security violation. The risks related to information security are mostly of a cumulative nature, which means that the possibility of an event occurring on a particular day or at a particular time may be quite small, but the likelihood increases with time. For instance, if an insecure password is chosen by an individual, there is a very small possibility that this non-adherence to procedure may be misused on a given day; however, this chance increases over time (Parsons et al., 2010).

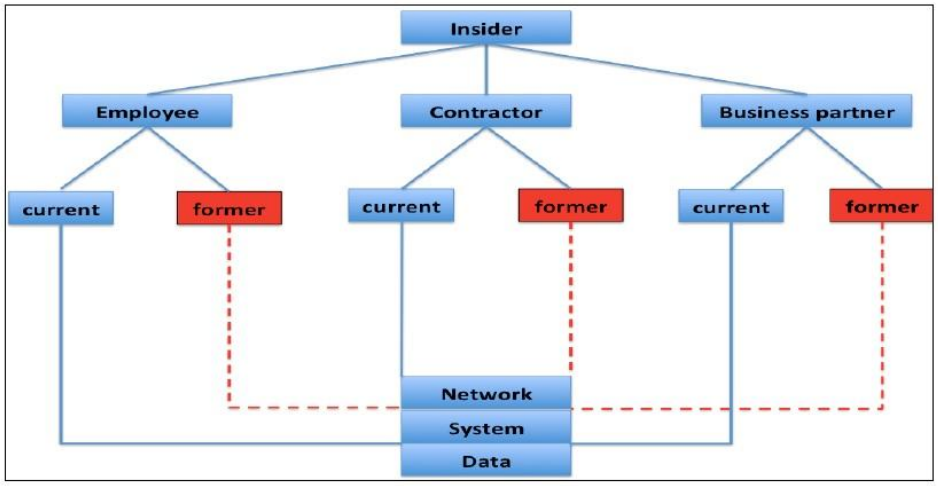
2.3 Insider Threats in an Organization

An insider is described by CERT as "an existing or ex-employee, contractor or other business partner who is or was previously authorized to access the network, data or systems of an organization".

They may are the company executives, regular employees, managers, board members, IT staff, consultants, contractors, outsources or even business partners (Wesley, 2009).

Cornelissen (2009) stated that there are several important attributes that differentiate between insiders and outsiders, including the following:

1. Trust: Insiders are usually those individuals who are trusted by the organization and their stakeholders. They are typically employees, but may also be consultants and contractors, temporary helpers or even people from third-party business partners who have a formal or informal business association with the organization (Schultz, 2002).
2. Access: Usually, insiders can legitimately access organizational resources. Here, it is important to differentiate between having legitimate access and authorized access (Brackney & Anderson, 2004).
3. Knowledge and skills: Typically, insiders have a privileged status in that they have knowledge about the information, services and systems employed in organizations (Wood, 2000). Since insiders have this kind of knowledge, breaches are more difficult to identify if it is the insiders violating policies (Wesley, 2009). The definition of insider is presented in Figure 2.2.



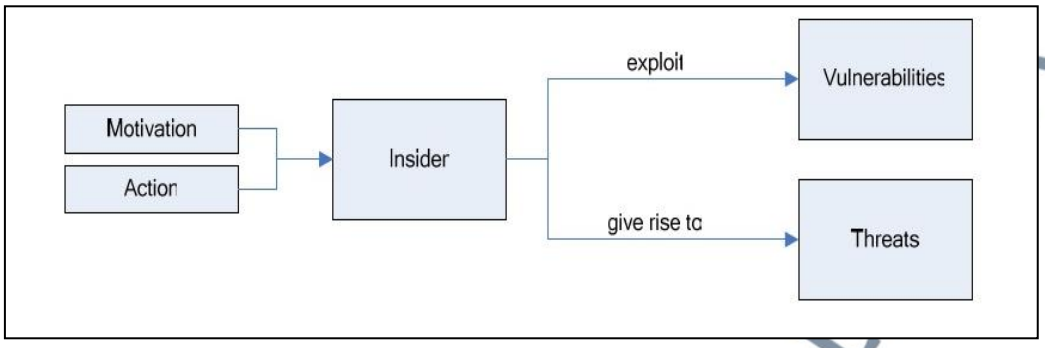
Source: Tuor et al., (2017)

Figure 2. 2: Insider Definition

Insider threat refers to attacks that are carried out from within the organization by the individuals who have either intentionally or unintentionally harmed organizational assets. Some examples of the intentional insider attacks are sabotage, embezzlement, espionage and exploitation of personally identifiable information. The kinds of assets that are attacked include source code, customer information, trade secrets, business plans, proprietary software and internal business information (Law, 2011).

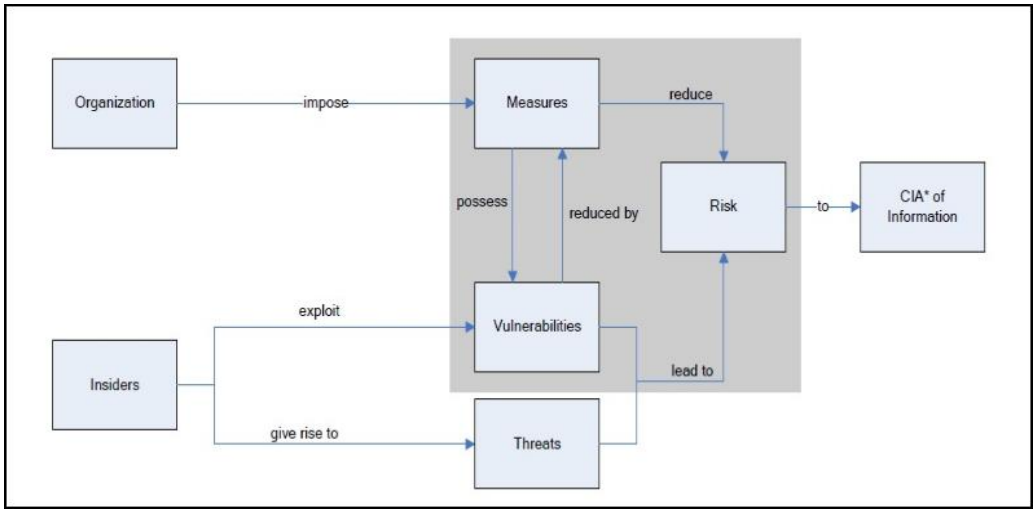
Organizations frequently incur greater losses from insider attacks. Insider threat serves as a major cause of financial and reputation risk to physical and intellectual property (Law, 2011). Four main areas that are vulnerable to insider threat were recognized by Deloitte UK (Law, 2011). These were:

1. Harm to critical assets and equipment;
2. Theft of critical assets and equipment;
3. Substantial removal or corrupting of files and records;
4. Releasing or leaking sensitive information. The attributes of insider threat are demonstrated in Figure 2.3.



Source: (Albert & Dorofee, 2001)

Figure 2. 3: Insider threat characteristics



Source: Wesley (2009)

Figure 2. 4: Conceptual model of the insider threat problem

2.3.1 Difference Between Internal and External Threats

External threats are the malicious activities that outsiders carry out intentionally. These outsiders may be located at any place across the globe and do not have legitimate access to organizational resources. External threats are carried out by a group of individuals or rival companies and are referred to as hackers. The motive of carrying out most of the external threats is to achieve financial gains or revenge (Aeran, 2006). Just like insider threats, external threats attack vital assets of the

organization, which may be the stored data, confidential documents or computer assets.

Excellent technical skills or social engineering are required to carry out external threats. On the contrary, such skills are not necessary for insider threats. Lack of knowledge is the reason for most threats that occur accidentally (Contos, 2006).

According to (Contos, 2006), "Insider threats are more difficult to address than external threats. Individuals perpetrating the crime are friends and co-workers which makes it difficult to identify the criminal. It instead makes the investigators think about the efficiency of security system." External threats are easier to prevent, control and identify. In order to access the systems of an organization, outsider has to bypass the security devices (such as firewall and IDS) that connects external network (internet) to the internal network of the organization. As this is a single point of contact between internal and external networks, it is easier to manage. Security devices are installed at this point of contact and monitor all the traffic that passes through them. In addition, methods utilized for attacking systems are familiar to us due to several incidents that have occurred in the past (Aeran, 2006). Table 2.1 shows the difference between internal and external threats.

Table 2. 1: The difference Between Internal and External Threats

Internal Threats	External Threats
Harmful activities that are carried out by employees either intentionally or unintentionally.	Harmful activities that are carried out by outsiders intentionally.
Organizational resources can be legitimately accessed by the attackers.	Organizational resources are not legitimately accessible for the attackers.
The critical organizational assets are targeted.	The critical organizational assets are targeted.
Fine skills are not required.	Fine technical skills or social engineering are required.
Carried out within the organization with the aim of modifying, stealing or harming the organizational assets, and may be accidental.	Carried out by externally infiltrating the organizational network to alter, steal or damage the organizational assets.
Insider threats cannot be curtailed with security controls.	Organizations can use the security controls in place to reduce the threats.
Insiders know about the target. They can legitimately access the resources that are not being monitored by any security device.	External attackers do not know about their target and need to acquire information and find out loopholes to get into the network.

There are limitations in the security solutions available to provide protection against insider threats. It is quite easy for the attackers to avoid being identified.	It is easier to identify external threats because the security devices can identify network probing.

2.3.2 Motives behind Insider Threat

There are several insiders, and so it is useful to take into account those that had the intention to do harm, as well as those that did not have any intention to do harm, but still carried out, or neglected to carry out, any action that caused harm to the organization (Noonan & Archuleta,2008).

Insider threat may be carried out by a displeased employee seeking revenge from the organization. Employees may also spy on company activities so as to acquire financial gains (Aeran, 2009). Undoubtedly, the reason for the occurrence of unintentional insider threat incidents is that the victim has not acquired security awareness training, does not fully comprehend organization security policy, is facing high job pressure, handles challenging tasks with inadequate knowledge, works with poor management systems and makes use of drugs (Greitzer et al.,2014) (Buckley et al., 2015).

According to (CERT, 2013), features of Intentional Insiders: -

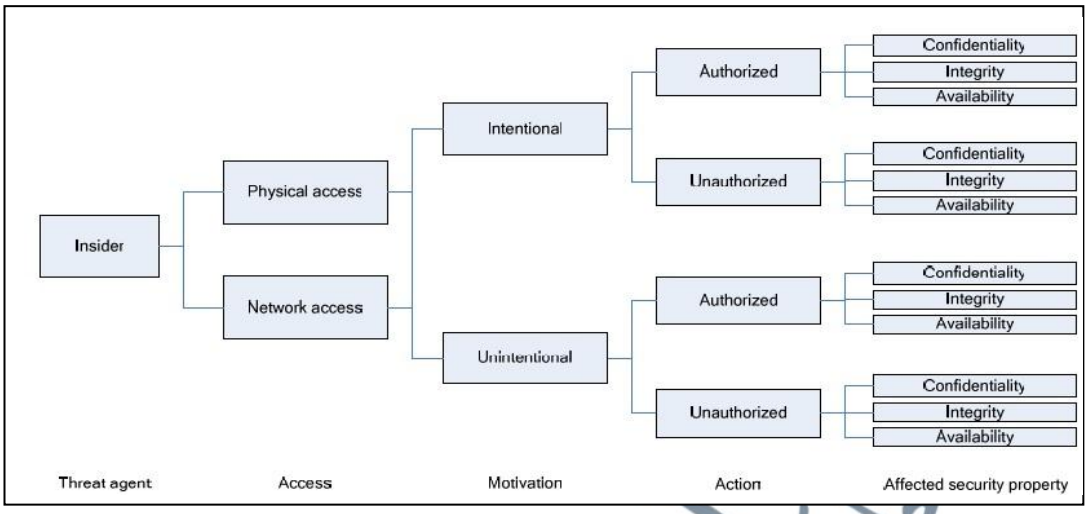
1. Is at a certain position or level in the organization.

2. Has or previously had legitimate access to the network, data or system of an organization.

3. Suffers from financial issues or experiences major personal or work-related pressure.

4. Is frequently working at odd hours.

5. Deliberately has a negative impact on the integrity, availability or confidentiality of the organization's information or information systems.



Source: (Albert & Dorofee, 2001)

Figure 2. 5: Insider Threat profiles

2.4 Unintentional Insider Threats

Those with no malicious intentions can also cause damage to the organization, either by their action or their inactivity, even when they break a rule knowingly. For example, a security guard who is not checking badges properly has no intention to allow a malicious actor to enter the building; however, he allows a person to come in who goes on to put the building on fire) (Greitzer et al, 2014).

Unintentional insider threat was described by CERT (2013) as: an existing or past employee, business partner or contractor, who is or was authorized to access the network, data or system of an organization, and who through action or inaction, harms, or significantly increases the chances of harm in the future, the integrity, confidentiality or availability of the organization's information or information systems without malicious intention.

2.4.1 Features of Unintentional Insiders

Some of the UIT features were identified by the CERT (2013) team as follows:

1. An existing or past employee, business partner or contractor: the insider who has been delegated some aspects of the task by the leader.
2. Is or was authorized to access the network, data or system of an organization: providing authorized access to the insider during the delegation process.
3. Action or inaction without malicious intention: non-malicious, weak performance shown by the insider
4. Adversely affects the integrity, confidentiality or availability of the organization's information or information systems: the task being unsuccessful.

2.4.2 Categories of Unintentional Insider Threats

CERT (2013) states that there are four major types of UIT threat vectors, and on the basis of the threat vector, four patterns of incidents can be determined.

Table 2. 2: Categories of UIT Threat Vectors

Threat	UIT threat vectors
1	• UIT-HACK, or malicious code (UIT-HACKing, malware/spyware), which is an outsider's electronic entry gained through social engineering (e.g., Unauthorized Access, planted or unauthorized USB drive, ID Theft/phishing email attack) and performed through a software, such as malware and spyware.
2	• DISC, or accidental disclosure (e.g., through the internet), where sensitive information is publicly displayed on a website, not handled property or sent to a wrong party through mail, email or fax.
3	• PHYS, or incorrect or accidental disposal of physical records – lost, stolen or discarded non-electronic records, like paper documents
4	• PORT, or portable equipment that is not possessed anymore – lost, stolen or discarded data storage device, like PDA, laptop, portable memory device, smartphone, hard drive, CD or data tape.

In general, the DISC, PHYS and PORT threat vectors are related to situations that arise due to an action (or lack of suitable action) carried out by a non-malicious insider. However, the UIT-HACK threat vector occurs due to an outside agent, i.e., it is an external threat. UIT-HACK cases would be classified as insider threat when it is facilitated by unintentional action or inaction of an internal employee. UIT cases that

occur due to actions carried out by the non-malicious insider alone are distinct from UIT cases that occur due to actions of an outside malicious agent as well as a non-malicious insider, e.g., an employee unknowingly becomes involved in social engineering. Insider threats taxonomy is presented in Figure 2.6, where the field of interest of this study is highlighted.

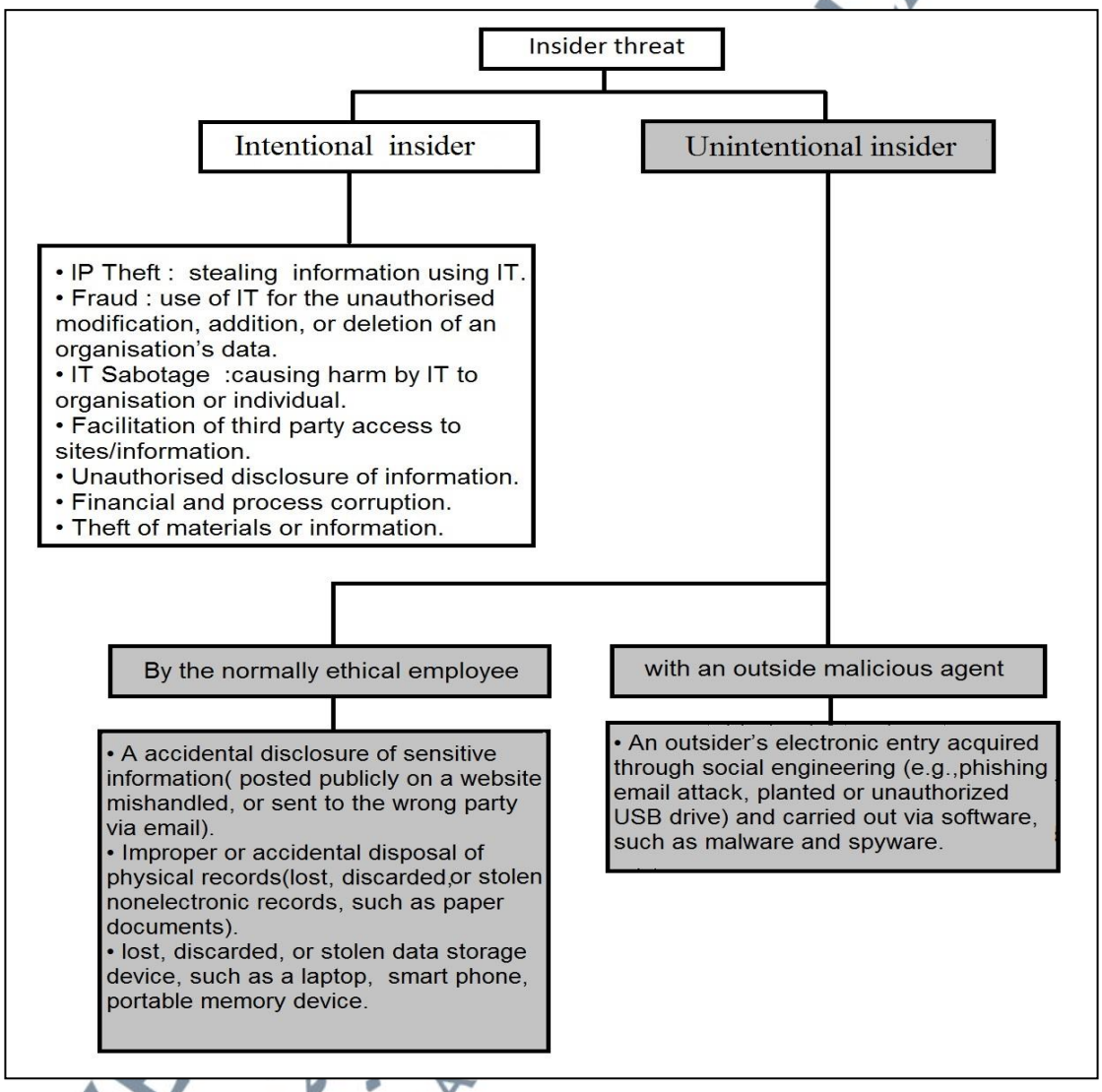


Figure 2. 6: Insider Threats Taxonomy (The Branch of Interest of the Study Highlighted)

2.5 Contributing Factors of Unintentional Insider Threat

The two major categories of UIT Contributing Factors obtained from the literature are shown in Figure 2.7, which the direct and the indirect factors. Direct

factors mostly rely on specific individual attributes and affect UIT to a significant extent. Indirect factors depend to a large extent on external factors like organizational issues (such as insufficient budget or budget management and security policy implementation). They also have an impact on direct factors and consequently, the employee. Each of these factors is examined in this section. In this research, all contributing factors of UIT, direct and indirect been considered. Where a comprehensive review of these factors was conducted from the literature due to their importance and their role in the occurrence of UITs, in order to be considered and focus on them while proposing countermeasures and to highlight them in order to be taken into account in the SMEs.

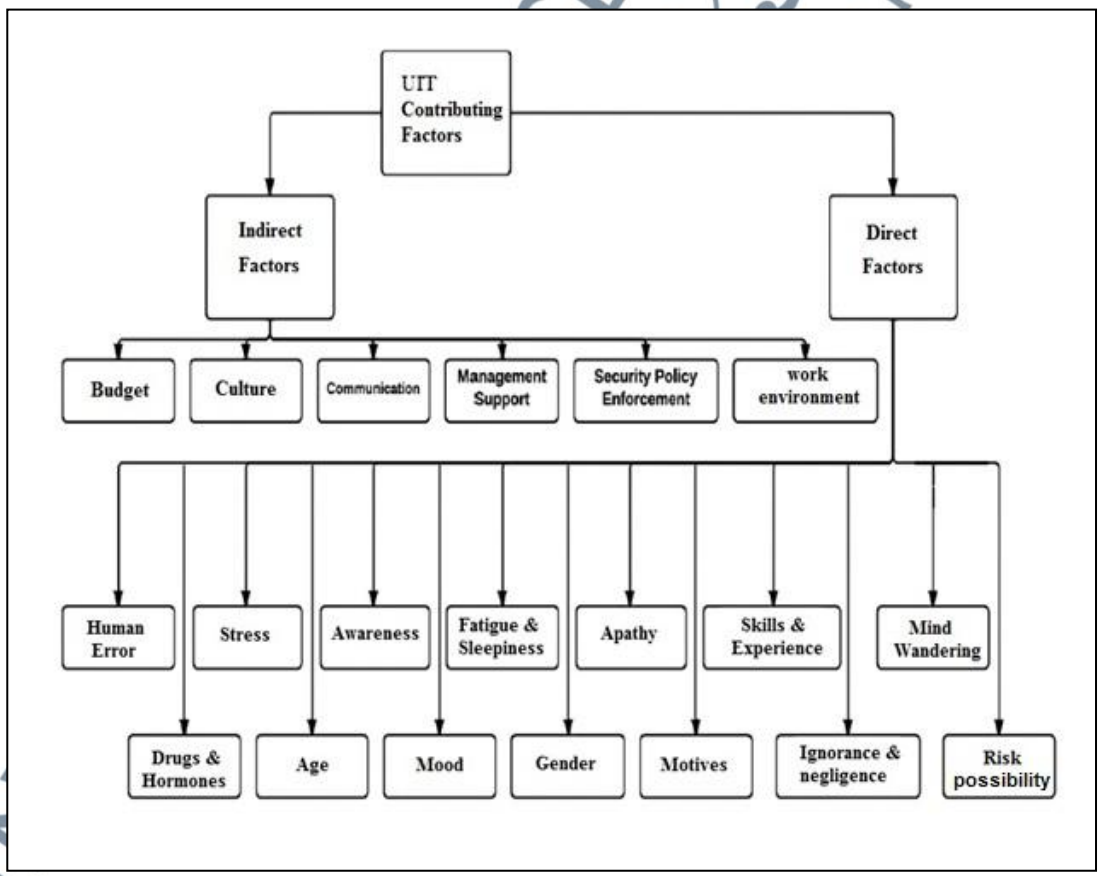


Figure 2. 7: Contributing Factors of UIT Extracted from Literatures

2.5.1 Direct Factors

Direct factors depend on the attributes of those individuals that directly affect the organization's Information System. These include human factors and performance indicators, like apathy, error, stress, experience and awareness, which are directly linked to the individual's personality and nature. These factors influence the organization's information system because of their direct impact on the individuals.

A. Human Error

Human error is typically the consequence or symptom of deeper issues. Human error is linked to the features of people's tools, operating environment and task (Dekker, 2002).

Human errors are responsible for around 80% of the accidents, ranging from air transport operations to nuclear power plants. Since the 1960s, there has been a steady increase in this percentage because of factors like higher system complexity and better error analytical techniques that improve our ability to detect errors (Hollnagle, 1993). Error may indicate a divergence in a system that is working perfectly otherwise (Avižienis et al, 2004). Human errors that lead to adverse effects are frequently outcomes of ineffective system conditions, individual employee attributes or process features, and hence, they are referred to as system induced human errors (Norman, 1983). If a ladder has to be used in a job, an error may lead to an accident; if sensitive, proprietary or classified information needs to be handled as part of a job, then an error may cause a security incident or breach of information (Pond & Leifheit, 2003).

Though it is not possible to fully eliminate human errors, it is possible to significantly decrease external influences by employing human error mitigation methods that concentrate on the system conditions that carried out, or possibly made

inevitable, the ensuing errors and negative results. When the underlying, contributing factors that cause employees to act erroneously are not identified and regulated, we face the risk of causing them repeatedly. In the cognitive domain, contributing factors to human error comprise of fatigue, mind wandering, lack of (or loss of) situational awareness and high subjective mental work pressure. Furthermore, the human error percentage can be affected by emotional states, both normal as well as abnormal (Dekker, 2002).

Information security events frequently occur when a security measure has been used that is adequate, but not affected by human behaviour. For instance, password validation policies instruct people to select a difficult password. This kind of password would possibly be a combination of letters, having at least one capital letter and digits that may be difficult for users to remember. This is why some people note down their passwords in unsafe places, e.g., their notebooks, which are easily accessible to other (Kraemer & Carayon, 2006) (Besnard & Arief, 2004).

A few errors are blunders or lapses, frequently "actions that had not been planned" or unintentional actions. Other errors comprise of mistakes or errors of decisions or judgement, where the "intended actions are not right", i.e., when one performs a wrong action, considering it to be right (HSE, 1999). UIT errors or blunders may be unintentional acts ("I did not mean to do that"), unintentional failures to take action ("I forgot to do that"), intentional but incorrect actions ("I thought I was supposed to do that"), intentional but incorrect failures to take action ("I did not know I was supposed to do that") (Greitzer et al, 2014).

B. Fatigue and Sleepiness

The FAA shows particular interest in how fatigues affect pilot performance as fatigue has been reported as a causal factor in various airline incidents. Changing time zones can lead to sleepiness in pilots (Kryger et al., 1994, Rosekind et al., 1994). Fatigue levels can also be affected negatively by shift work (Akerstedt 1998, Gander et al., 1998), especially evening shifts (Signal et al., 2006).

Greater rates of human error with higher overall sleep loss during rotating shifts was found by Gander (Gander et al., 2008). It has been shown in several studies that performance is inversely related to subjective experiences of sleepiness in sleep-deprived rail engineers (Gander et al., 2002), F-117A pilots who were compelled to stay awake for 37 hours (Caldwell et al., 2003) and commercial airline pilots (Co et al.,1999). The ensuing performance is influenced by the degree of fatigue. It was found in a study of airline pilots that with an increase in fatigue, their behaviour starts becoming less accurate, they are more willing to accept a lower standard of performance, and their attention decreases to such an extent that they have lower possibility of adhering to a peripheral-vision information required for safe flight (Caldwell et al., 2003). There is a decrease in the frequency of social engagement between pilots and co-pilots (Caldwell, 2012). With an increase in fatigue, the consistency of performance keeps decreasing (Dinges, 1990), and pilots frequently go to sleep, due to which they miss task-related details that are critical for problem-solving (Caldwell, 2012).

When employees in a computing environment feel sleepy, either due to jet lag, changes in the circadian rhythm or because of shift work, they may show less attentiveness and exhibit highly inappropriate reactions to critical network security information (Greitzer et al, 2014).

C. Stress and Subjective Mental Workload

Subjective mental workload refers to the internal feeling of being mentally burdened with the work experience (Lupien et al., 2007). Subjective mental workload is also defined with respect to stress, and there are various ways in which stress is linked to human error (Huey & Wickens, 1993). Stress decreases attention (Houston, 1969, Stokes & Kite, 1994) in a way that peripheral information has lower chances of being attended to in high-stress situations (Weltman et al., 1971). In addition, stress decreases the capacity of working memory in a way that limited information can be held in memory at a single point in time (Davies & Parasuraman, 1982; Hockey 1986; Wachtel 1968). When there is excessive subjective mental workload, people may decrease the threshold of acceptable performance, which would bring a decrease in performance. In addition, they would seek less demanding and more efficient ways of carrying out the same tasks, strategically avoid carrying out particular tasks (i.e., the lower priority tasks), or not carry out critical tasks (Hart & Wickens, 1990). Heavy work burdens and stringent project deadlines can lead to individuals being stressed in the work settings. People exhibit maladaptive reactions to stress and work overload. Stress gives rise to human errors. Those with stress are likely to bypass Information Security policies. There is a direct correlation between stress and fatigue and Information security vulnerabilities (Carstens et al, 2004).

Stress and additional burden are created for employees with unbalanced and excessive workloads; this kind of burden substantially decreases the morale of the employees and the organizational ethics (Kabay, 2002). When significant workloads are assigned to the employees, they are placed under additional and unwanted pressure, which can cause a decrease in the organization's moral behaviour. It is this moral and ethical breakdown that gives rise to Information Security incidents as

people feel undervalued. It is vital for organizations to ensure that their employees are not affected by internal as well as external pressures (Kabay, 2002).

D. Situation Awareness

Situational awareness (SA) is described by Endsley (1995) as "the view regarding the elements in the environment in a given time and space, understanding their meaning, and presenting their status in the impending future. It signifies a state of knowledge regarding a specific environment". In general, it is determined that effective decision making to decrease error rates is considered to have a good SA (Endsley & Rodgers, 2000). To use finite memory in the best way and take significant, timely decisions in a dynamic environment, it is essential for operators to understand and handle specific information, while eliminating unnecessary information (Princ & Salas, 2000).

Case studies of significant airline accidents were examined in a study, which showed that in dynamic environments, information that is required to enhance SA was not being considered. This was despite the fact that pilots were instructed through checklists to assess instrumental panels to obtain the information required for appropriate SA (Endsley & Rodgers, 2000).

In the field of computing, inaccurate or incomplete SA at any particular time may give rise to human error that leads to system failures, which brings about a possible increase in organizational risk. Employees should be aware of the attack vectors being employed in the present times. If one fails to foresee a phishing campaign, network security will be compromised (Greitzer et al, 2014). It is ensured by the awareness programs that the employees comprehend their responsibilities and are central parts of Information Security System. For example, if users get any

suspicious email, they should report it immediately. Information security awareness terminology is related to the way people comprehend and are aware of an Information Security System by security policy. It is possible to misunderstand security policy; hence, a vital part is played by the awareness program, similar to Information Security process (Greitzer et al, 2014). It is widely accepted that there is a positive effect of awareness programs on the effectiveness of Information Security System (Kraemer & Carayon, 2006) (Redmill, 2002). It was found in the earlier studies (Greitzer et al, 2014; Forcepoint, 2016; Brian & Christiansen, 2009) that awareness factor was a very significant contributing factor of UIT.

E. Skills and Experience

The function of role is facilitated by skills, which performs a vital part in humans exhibiting effective performance. In addition, education and training also play a critical part in formulating skills and exhibiting a commitment to maintain professionalism and proficiency. Skills are a significant force in handling Information Security issues, like incident response (Werlinger, et al, 2009). There is a lack of adequately skilled staff, because of which information security policy exhibits weak performance (Kraemer & Carayon, 2006). A significant part is also played by skill competency in handling all elements of an information security system (Lee& Lee, 2002). A lack of awareness among individuals regarding how to address suspicious emails may cause them to open such emails (Herzog, 2010).

Organizations should not concentrate entirely on individuals who are entirely technological competent. Training programs should be formulated on the basis of mixed and varied factors of business so that employees acquire the skills needed to face information security challenges and fulfil organizational objectives (Briggs et al.,

2006). This is more important when there are rapid changes in business behaviour because of latest technological developments (Leek et al., 2003).

F. Mind Wandering

The process in which our attention diverts from the immediate task at hand and because of which we become absent-minded is referred to as mind wandering (Smallwood & Schooler, 2006). Mind wandering may have a negative impact on cognitive processes and behaviour al responses (James, 1892). This makes task-relevant memories inaccurate (Smallwood et al., 2003). In the same way, off-task thinking is linked to delays in responses, and also greater rates of making inaccurate response (Cheyne et al., 2006; Smallwood et al., 2007).

Sometimes, errors occur because of lapses or blunders, frequently unintentional actions or "actions that did not go as planned". These errors occur during a known task, and involve slips (for example, pressing an incorrect button or reading the wrong gauge) and blunders (for example, forgetting a vital step in a procedure). It is common to experience such errors in highly trained processes, where the individual does not have to fully concentrate on their tasks. It is not possible to eliminate such errors by training; however, better design can decrease the chances of such errors occurring and offer a more error-tolerant system (NOPSEMA, 2018). In general, when such errors take place, the individual has the relevant skills, knowledge and experience to perform the task accurately. They occur when the tasks have become more mundane and less unique, such as swapping digits when copying numbers (for example writing 0.31 rather than 0.13) (NOPSEMA, 2018).

G. Apathy

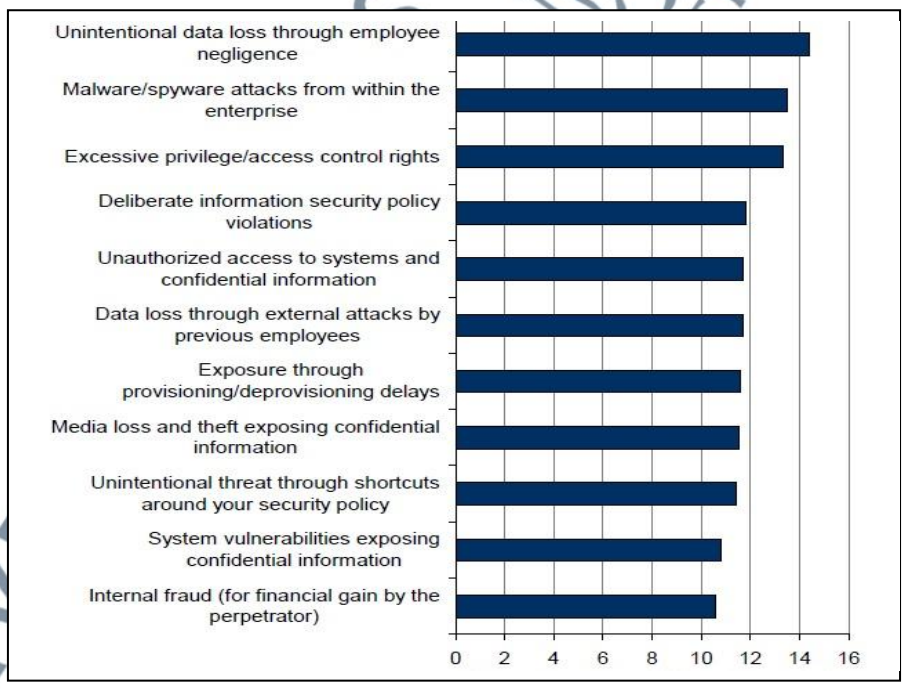
Apathy in an organization refers to the lack of willingness of employees to perform their role in attaining organizational goals and objectives when they should be exhibiting pro-social behaviour, and also their unwillingness to execute organizational procedures (Thomson & Niekerk, 2012). A positive attitude, optimal working conditions and motivation help in exhibiting better performance, while apathy and unresponsiveness give rise to undesirable performance (Bartol & Martin, 1994). It is asserted by Thompson that when there is miscommunication between employees and senior management, misunderstanding is created, which gives rise to employee apathy (Thomson & Niekerk, 2012). It is also found in this study that employees feel frustrated and disgruntled in those organizations that have a coercive environment (Layton, 2005; Schein, 1999). A coercive environment in an organization is one in which everything is dictated to the employees and they are not consulted when formulating corporate goals and objectives. The employees in such environments feel a lack of motivation to work towards attaining organizational objectives, like Information Security System objectives. For instance, if senior management modifies backup processes without taking into account human and organizational limitations, a coercive environment will be created in which employees show a lack of motivation to adhere to the security policy. Eventually, the team's performance deteriorates and the proposed Information Security System will not be effective as desired (Schein, 1999).

H. Ignorance and Negligence

Employees in organizations often unintentionally do not follow security policy (Vroom & Solms, 2004). There are differences between violations (non-compliances,

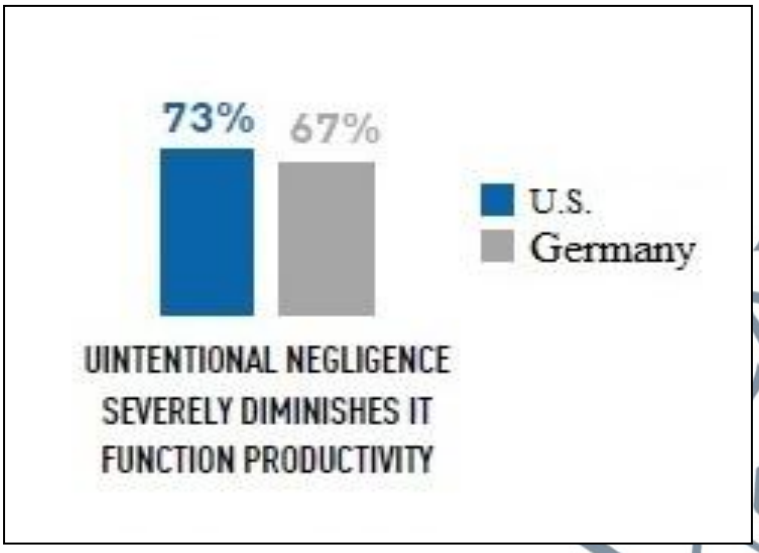
shortcuts, circumventions and work-arounds) and other threats in that violations are intentional, but typically well-defined failures where the employee intentionally does not perform the function properly (HSE, 1999).

The effect of ignorance or carelessness on an Information Security System calls for decisive action and information security professionals should manage this issue. To address this issue, a few authors suggested employing the deterrence theory that recommends the threat of sanction (Parker, 1999; Bequai., 1998; Tudor, 2001; Kankanhalli et al, 2003). However, it is asserted by Vance (2010) that fear or threat cannot always rectify employee negligence and/or ignorance of Information Security policies. There are different contributing factors of UIT, with the greatest proportion of accidental issues arising due to negligence and ignorance (Forcepoint, 2015; Brian & Christiansen, 2009; Forcepoint; 2016; orcepoint, 2016).



Source: (Brian & Christiansen, 2009)

Figure 2. 8: Average Number of Internal Incidents per Year



Source: Forcepoint (2016)

Figure 2. 9: Negligence percentage among Insider Threats

I. Motivation and Incentive and Disincentive Policy

Good behaviour is rewarded and improper behaviour is punished through the incentive and disincentive policies in organizations. There are a few links between people's attitudes and incentives and disincentives policies; even a small amount of persuasion brings about an increase in motivation. According to Kabay, organizations should seriously consider even a simple comment made by an employee on Information Security policy as it can eventually have an impact on the entire Information Security System in the organization (Kabay, 2002). Though incentives and disincentives are vital factors in organizations, they have not been examined in earlier studies on Information Security Systems. These factors influence the motivation of employees to follow Information Security policies (Thomson & Niekerk, 2012).

At times, the focus of organizations is on punishment when it should be on training and reward policy. For instance, organizations should reward those employees that report Information Security breaches or dubious behaviour and providing training

to people rather than punishing them when they view personal emails at work. Incentives serve as an encouragement to employees to exhibit a positive attitude and act pro-socially, whereas punishments estrange them. Employees may continue to adhere to Information Security policy even when they do not approve of it because of the reward they receive for exhibiting the required behaviour (Layton, 2005; Schein, 1999).

J. Risk Possibility as Personality Feature

Examining an employee's risk propensity (readiness to take risks) may support the organization's effort to recognize and eliminate contributing factors to UIT. The Balloon Analogue Risk Task (BART) may be used to measure risk propensity, which is a computerized, laboratory-based method that consists of risky behaviour, where, similar to actual situations, risk is rewarded to an extent, following which additional risk leads to weaker outcomes (Greitzer et al., 2010).

According to the findings, the BART results are related to risk taking over a given time period (White et al., 2008) and can predict risk-taking behaviour s, such as use of alcohol and drugs, and smoking cigarette (Lejuez et al., 2003), aggression, theft, gambling, disinhibition, psychopathy and impulsivity (Hunt et al., 2005). It was also found by Nicholson and colleagues that personality is related to risk-taking behaviour (Nicholson et al., 2005). Therefore, individuals' predisposition to take risks may be explained by personality traits.

The potential relationship between personality traits and individuals at risk of turning into insider threats was evaluated by (Greitzer et al., 2014) and (Brown et al., 2013).

K. Gender

A relationship between gender and risk perceptions and between gender and risk taking has been found in earlier studies. Over 150 studies that examined the risk-taking behaviour of male and female participants were reviewed by Byrnes, Miller, and Shafer, and the findings showed that men "are more likely than women to take risks" (Byrnes et al., 1999). According to Courtenay, there is greater likelihood of males belonging to all age groups to be involved in over 30 behaviour s that increases their risk of disease, injury and death compared to the female participants (Courtenay, 2000). It has been shown in BART testing that compared to women; men are more likely to be involved risky behaviour (Hunt et al., 2005).

The variations in risk perception between male and female are not related to education or rationality (Gardner & Gould, 1989). Furthermore, men and women consider risky situations in different ways (Figner& Weber, 2011).

A relationship between gender and risk-taking behaviour was also established by Greitzer et al. (2014) in the field of cybersecurity, and specifically in terms of UIT in the workplace.

L. Mood

There has been inconsistent research seeking to examine the impact of mood on taking risky decisions. A mood-maintenance hypothesis was formulated by (Isen et al., 1988), according to which individuals in a negative mood have a tendency to take higher risks compared to those who are in a neutral or positive mood, and that risk-taking enhances their overall mood.

The opposite is asserted in other studies, e.g., those by Bless and colleagues, and Au, arguing that a more comprehensive processing and information gathering is exhibited by individuals when they are in negative mood compared to when they are in a positive mood (Bless et al., 1990; Au et al., 2003). According to other studies, when individuals are in a positive mood instead of a neutral mood, they would be more appropriately risk averse when a potential loss was understood as being significant or real (Isen et al.,1988; Nygren et al., 1996).

M. Age Effects

Risk tolerance changes with time in individuals and also in societies. There is lower perception of risk in young drivers as compared to the older drivers (Ivers, 2009). This is considered by car insurance companies when establishing insurance premiums for young male drivers (Esurance, 2013). The increase in risk perception threshold will be directly linked to the time duration for which a person is exposed to a risk, just like the Stockholm syndrome (Carver, 2008; Fabrique et al., 2007).

Risk assessment should be considered as a continuous process, and there should be full re-assessment of risk from time to time so that the impact of decreased perceived risk threshold over time can be prevented (Greitzer et al., 2014).

N. Influence of Drugs and Hormones

A drug is capable of decreasing the risk threshold of an individual by decreasing inhibition or risk perception sensitivity. Several risks are related to drugs and alcohol overuse, such as loss of productivity, financial issues and not being successful at school (HealthyPeople.gov, 2013). The results of a study showed that “approximately 17% of 18- to 20-year-old drove under the influence of alcohol last year”, which is a

possible reason for a decreased threshold of risk-taking because of the effect of alcohol (Stagman et al., 2011). Participants who had taken five or more drinks on a single occasion were less likely to use condoms, thus making it more likely for them to contract a sexually transmitted disease (Graves, 1995).

The number of risks taken by people is also affected by hormones, especially dopamine, which is the "feel-good chemical" in the brain (Park, 2008). Zald et al. (2008) found in their study that there is high prevalence of dopamine in the brains of risk-takers, or they have lesser dopamine-inhibiting receptors. The authors deduced that individuals with greater levels of dopamine have higher tendency to take risks, like abusing drugs and exhibiting other unsafe behaviour s.

A drug-free environment should be encouraged through drug education and reforms (no tolerance and rehabilitation programs that can be accessed in employee assistance programs (EAPs)) so that risk-taking behaviour because of drug use is decreased (Greitzer et al, 2014).

2.5.2 Indirect Factors

There is an impact of indirect factors on direct factors as well as on information system security. Such factors have an impact on people through aspects regulated by organizations and which individuals cannot control, for example culture, budget and communication.

A. Budget

An organization needs money to run its operations. Information security experts are of the view that budgets significantly affect the efficiency of Information Security Systems. The need for training arises when stressing on the dimension of cost

effectiveness. Training programs that are not very costly are needed for certain cost-reducing measures, like automated user access provisioning. This shows how budget planning is related to direct human factors (Al-Awadi & Renaud, 2007; Bazavan & Lim, 2007). To make sure that an Information Security System effectively attains its objectives organizations should adopt an effective cost strategy for handling the technical and personal requirements of the Information Security System. For example, if an access control system has not been adopted or if employees are not getting sufficient training, then the organizations will not be able to accomplish their Information Security System objectives adequately. It is imperative for organizations to make investments in information security; however, they may not be able to sustain a suitable level of investment, which is why they should mainly concentrate on those areas that are most vulnerable and threatened, for example back-up and disaster recovery planning (Bazavan & Lim, 2007; Islam & Falcarin, 2011).

B. Culture

Individuals' security behaviour can be affected by group norms. Individuals typically adhere to group norms, and hence, if information security is considered as a crucial and serious problem by the group, then there is greater likelihood of the individuals within that group valuing and adhering to the security policies. On the other hand, if the group accepts risk-taking, then there are greater chances of risks being taken.

Sharing passwords is considered as an indication of trust in a colleague, and hence, if people are not willing to share a password, it may be considered as a sign of lack of trust in their colleagues. The prevalence of such norms in an organization calls for extensive education to modify this behaviour (Parsons et al., 2010). A fresh

employee may see that there are a few employees and also some managers that do not adhere to the security policies imposed by the organization, and this has an impact on the perceived risk thresholds of the employee (Clifford & Marcus, 1986). It is vital to consider information security culture (ISC) as a significant factor for risk tolerance and decision-making in the organization (Boholm 2003; Douglas, 1992; Douglas& Wildavsky, 1982). Values, beliefs, attitudes, reputation, practices and ethics form the ISC of an organization and its employees. ISC presents a behaviour al model that enables organizations to secure information assets (Dhillon & Backhouse, 2001). Management support is required for ensuring that ISC is upheld so that there is an increase in the employees' adherence to the security policy. This can be accomplished by increasing awareness through training and education programs (Lim et al., 2010). It is also essential to consider ISC as a contributing factor in decrease cybersecurity threat. Risks may be decreased through culturally informed strategies (Reza et al., 2013).

C. Communication

In an organizational context, communication signifies the exchange messages and ideas between people within and outside an organization. People can deliver a message to a suitable destination or individual through communication. A vital role has been performed by the development of information and communication technology in the field of computer security (Dhillon & Backhouse., 2001).

There are various types of communication; with the most common being face-to-face and written, electronically and with hand. Communication helps in improving Information Security awareness and encourages employees to conform to the security policy. However, if communication is not carried out properly or is misused, the

Information Security System would be adversely affected. Management should communicate effectively with employees to make sure that they know about Information Security policy and comprehend why it is important to effectively implement it. Subsequently, effective communication involves reaching all employees within an organization at all of its hierarchical levels (Pattinson & Anderson, 2007).

Communication includes security awareness workshops and also phone, email and face-to-face meetings. Confidentially plays a vital role in email exchanges among employees within an organization and with those in other organizations. Employees should know about the kind of information that can be given to third parties without causing a breach in confidentiality (Reza et al., 2016). Some indirect causes that give rise to UIT are data flow elements, like insufficient procedures and guidelines and weak communication.

D. Security Policy Enforcement

A security policy refers to an organization document that outlines information security processes and policies. It is vital for employees at different organization levels to comprehend the security policy and take part in its implementation in accordance with their position. A significant issue for an Information Security System is implementing a security policy, and management should ensure its effective implementation (Tipton & Krause, 2008; Ericsson, 2010) (Chenine et al, 2014).

Examples of factors that should be a part of security policy are access control, network security, password policy and IT personnel job descriptions (Vacca, 2012).

E. Management Support

Implementation of policies related to the ISS in organizations require management support throughout all stages, i.e., from the design stage to the evaluation stage. Management is not only supposed to advocate ISS, but also has to clearly explain Information Security Policy to the entire organization. Management can endorse an Information Security System in organizations by allocating a sufficient budget that is completely under the senior management's control. The senior management is of the view that an Information Security System is fully responsible for an IT department that needs to ensure that relevant and sufficient software systems are installed for the purpose of information security (Jordan & Fung, 2002). Full support of the senior management is required with respect to the budget and implementation of Information Security policy (Von, 1999). There are deep-rooted factors that give rise to human errors, like work setting (inadequate resources, inefficient management systems, distractions, insufficient security practices) and work planning/management (job pressure, task complexity, time factors, modifications in routine, weak task planning or management practice, inadequate skills, knowledge and ability) (Pond & Leifheit, 2003).

F. Design of Work Environment

Certain factors increase or decrease the probability of errors, like weak design, time pressure, distraction, work burden, competence, communication systems and noise levels). A weakly design activity may be at risk of facing various errors, which can be countered by redesigning the task or equipment (HSE, 1999). Weak layout and design of workplaces should be considered as a causal factor of UIT. It may be quite challenging to rectify a dangerous layout after it has been developed (Mansor et al.,

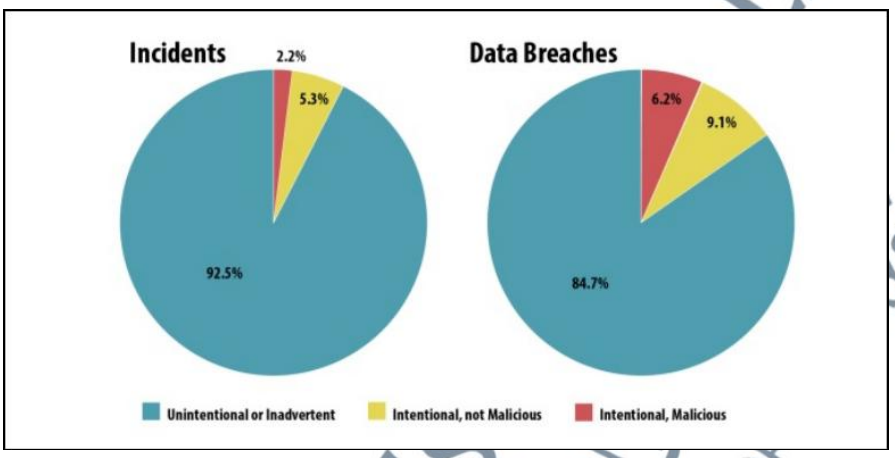
2011). It has been found that physical discomfort is related to worker distress and job discontentment (Murphy et al., 1986). Environmental interfaces are related to the physical environment (noise, vibration, illumination, temperature, etc.), facility layout and arrangement, workspace setting and environmental controls, particularly with respect to the way environmental factors affect human performance and safety and health. The issues in terms of environmental interfaces are that they give rise to fatigue and/or divert attention from the main task, which increases the possibility of human error (such as noisy environment where it is difficult to hear alarms, glare, suffocating workspace) (Greitzer et al., 2014). Information is a vital factor that influences the individual's ability to carry out the tasks assigned to them. Issues related to information include: too much information, intricate information, lack of information, incorrect information and weak flow of information (Jeffrey et al., 2002). When using a weak design and difficult to use technology and equipment, similar kinds of mistakes are made (Kerm et al, 2007). The fact that systems are designed for simplicity is a significant issue with systems design, because of which a person who is usually privacy-conscious may make incorrect security decisions (Bratus et al., 2008). The frequency with which human error occurs is often determined by system design and human interaction, specifically when there is a minor mismatch between the system design and the person using it. The ease and intricacy of systems and software design, font size and color that create optical dispersion, as well as uncomfortable office (noise, chaos in files and documents and lighting issues) can all have an impact on the person using the information system (Wood & Banks, 1993).

2.6 Likelihood and Consequences of Unintentional Insider Threats

The ransomware market became even bigger by 2020. The New York Times stated that there has been an increase in ransom demands in cities of Riviera Beach and Lake City that recently paid ransoms worth US$600,000 and US$500,000, respectively. Cybercriminals demanded a ransom of US$14 million from a Brazilian power company in July 2021 (Hettu, 2021).

It is believed by a large percentage of organizational security professionals that the greatest risk to their organization is UIT, with over 40% claiming that their biggest security concern is employees' accidentally harming their security (AlgoSec, 2013). A survey was carried out by Brian and Christian (2009) across the UK, the US, Germany and France. In this survey, eleven kinds of internal incidents occurring every year were examined. It was found that unintentional data loss caused the greatest number of incidents. On average, the organizations examined faced 14.4 incidents of unintentional data loss. Most of the organizations (52%) classified the incidents occurring due to insider threats as accidental. Around 19% of the organizations were of the view that the threat incidents were carried out intentionally, while 26% were of the view that they were an equal combination. The greatest number of unintentional data loss incidents occurred in the financial sector (13.7), followed by the public sector (14.5) and the healthcare sectors (14.5). Unintentional data loss through the negligence of employees is responsible for the highest financial impact in France. Nevertheless, an organization can still be adversely affected by unintentional data loss. The research showed that a high proportion of accidental issues were caused by contractors and temporary staff, which is not a surprising outcome. These individuals have just a causal understanding of the security policies of a firm. A high percentage of employees have mobile phones, laptops, different email accounts and access to

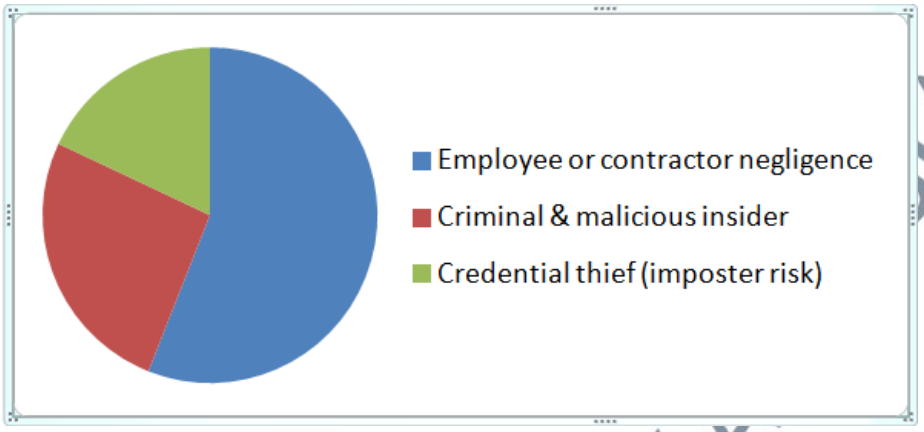
databases and applications, because of which dealing with insider threat becomes a major challenge. In addition, this situation generates significantly more risk for an organization due to accidental or ignorant actions compared to 1-3% of the insiders that exhibit malicious actions intentionally (Brian & Christiansen, 2009). The percentage of UIT accidents compared to other accidents is depicted in Figure 2.10.



Source: Sher-Jan (2018)

Figure 2. 10: Percentage of accidents

The negligent insider is the root cause of most incidents. A total of 3,807 attacks, or 56%, were caused by employee or contractor negligence, costing on average $484,931 per incident. This could be the result of a variety of factors, including not ensuring their devices are secured, not following the company's security policy, or forgetting to patch and upgrade (Ponemon, 2022). Figure 2.10 shows the distribution of accidents reported attacks analysed by (Ponemon, 2022).



Source: Ponemon (2022)

Figure 2. 11: The distribution of accidents reported attacks

The counts for malware identified by Microsoft's malicious software removal tool in the second half of 2011 were reported by Microsoft. This tool is operational on over 600 million machines worldwide.

The threat intelligence report by Microsoft stated that around 780,000 computers were infected by malware Family 1 and almost 400,000 computers with malware Family 2 in the second half of 2011. It was presumed by Microsoft's estimation approach that almost 44% of the infections needed some kind of user interaction to spread. If it is also presumed that none of the users knowingly installed the malware on their machines, there would still be 519,200 cases of UIT compromising a computer with malware from just the first two families.

Apart from these two malware families, 25 popular families of malware that were identified over 25,000 times each in the same 6 months were listed by Microsoft. The numbers are not accurate and a few assumptions had to be made. In addition, it may be extremely difficult to obtain a significant sample of data to make deductions regarding the entire population. It was found in the studies that the UIT problem is quite significant (Burke & Christiansen, 2009; Faulhaber, 2011).

The threats can cause a significant deletion/corruption of files and records, exposure and leakage of information as well as financial drawbacks and loss of reputation (Law, 2011). The consequences of human errors in information security include circulating incorrect or confidential information, disruption of information system, decreasing the integrity of information, considerable economic loss and lack of ability of provide services (Carstens et al., 2004).

The extent of the unintentional insider threat problem has been highlighted in various studies and surveys. Table 2.3 demonstrates the studies and surveys performed in this field between the years 2007 and 2021.

Table 2. 3: Summary of Studies and surveys on UITs (2007-2021)

Title\ Authors	Measurement Tool	Key Findings	Addressed factors
Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System\ Kumaraguru et al., (2007, a)	Experiment to teach people about phishing during their normal use of email.	- The report includes Carnegie Mellon University's Lori Cranor, who has performed a lot of work in this field and helped in attaining a spin-out.	•Situation awareness. •Skills and experience of employees.
Data Leakage Worldwide: Common Risks and Mistakes Employees Make\ Cisco Systems, White Paper. San Jose, (2008)	Surveys carried out among over 2000 employees and information technology professionals from 10 countries.	- The relationships between employee behaviour and data loss, and also IT perceptions of those factors are evaluated in the survey. The results showed that employees from all over the world are involved in behaviour s that compromise the security of corporate and personal data, that IT professionals frequently do not know about these behaviour s and that avoiding data leakage is a business-wide issue.	• Human error. •Situation awareness. •Skills and experience of employees. •Ignorance and negligence. • Risk possibility as personality feature.
Data Leakage Worldwide: The Effectiveness of Security Policies (2008) \ Nicolett Mark & Pescatore John	Surveys performed in 10 countries.	- The report discusses the impact of security policy creation, compliance and communication on data leakage. The results of the analysis show that inadequate security policies and insufficient conformance of employees to security policies	• Security policy enforcement.

		are major factors leading to data loss.	
Insider Risk Management: A Framework Approach to Internal Security\ (Burke & Christiansen,2009)	Survey including 400 respondents from organizations of different sizes.	- Most of the organizations (52%) classified incidents emerging from insider threats as being mostly accidental. It was determined in the study that only 19% were of the view that insider threat incidents were mainly deliberate and 26% were of the view that they were of an equal combination.	• Human error. •Stress and subjective mental workload. •Situation awareness. •Skills and experience of employees. •Ignorance and negligence. • Risk possibility as personality feature.
Verizon 2013, Data Breach Investigations Report\ A global study conducted by Verizon risk team.	Over 47,000 incidents were examined, 621 confirmed data violations were reviewed, as well as 19 international contributors.	- Unintentional actions tend to have the same impact of data violation. Over 47000 security incidents were presented in the report that included sufficient evidence of this fact. - These comprise of events like dispatching sensitive document to incorrect recipients and also system administrators and programmers making fewer recurring mistakes. For example, in a certain case from our caseload, an incorrectly configured application debug setting put sensitive financial data at risk and exposed it to unauthorized parties.	• Design of work environment. • Management Support. • Human error. • Stress and subjective mental workload. • Situation awareness. • Skills and experience of employees. • Ignorance and negligence. • Risk possibility as personality feature.
Employee negligence: The most overlooked vulnerability\ Bimal Parmar, (2013)	Surveys study	- Employee Negligence is the vulnerability ignored most often.	• Skills and experience of employees. • Ignorance and negligence. • Apathy. •Security Policy enforcement. • Management Support.
Insider Threats: The Danger Within. (IBM, 2017).	Surveys study in which 170 federal employees were studied.	- The results show that UITs are responsible for approximately 30% of all cyber security events occurring in government departments and organizations.	• Skills and experience of employees. • Management Support. • Security Policy enforcement. • Ignorance and negligence. • Apathy.
A Review on Insider Threat Status in Malaysian Organization (Isnin, & Sedek,2018)	Insider security incidents were reviewed.	- Results showed that 87% of all Malaysian web traffic is malware, and merely 0.2% emerged from Malaysia to worldwide networks.	• Management support. • Budget of organization.
Insight into Insiders	Literature	- Insider threats refer	• Ignorance and

and IT: A Survey of Insider Threat: Taxonomies, Analysis, Modeling, and Countermeasures (IVAN, et al, 2018).	review of 100 ranked papers in the domain, obtained from Google Scholar.	to one of the most challenging cybersecurity issues of the present times that have not been addressed adequately by commonly used security solutions.	negligence. • Motives and incentive and disincentive Policy. • Human error. • Situation awareness. • Apathy . • Risk possibility as personality feature. • Communication. • Culture. • Budget of organization. • Design of work environment. • Security policy enforcement.
ENISA Threat Landscape Report. 15 Top Cyber-Threats and Trends (The ENISA, 2018).	Surveys study.	Human factors or negligence caused 25% of the incidents of data violation.	• Skills and experience of employees. • Ignorance and negligence. •Apathy. • Security Policy enforcement. • Management Support.
Ponemon Institute, LLC. Security of Cloud Computing Providers Study (Ponemon Institute, 2020).	Surveys study.	- The number of incidents increased by 47% and there was also an increase in the average yearly cost of insider threats by 31%, increasing to $11.45 million in the last 2 years. - Though 61% of the employees believe that insider threat is highly risky, it was believed by just 44% that the company gives the highest priority to insider threat.	• Budget of organization. • Culture. • Communication. •Security policy enforcement. • Management support. • Situation awareness.
Insider Threats in Cybersecurity: The Enemy within the Gates. (Mazzarolo & Jurcut, 2020).	Literature review.	- Technical controls are already implemented in majority of the organizations' security programs in the present times. However, organizations cannot solely depend on them due to the highly threatening landscape. - The carelessness of unintentional actors can give rise to a significant security breach. This may lead to as much damage as that caused by malicious actors.	• Skills and experience of employees. • Ignorance and negligence. • Apathy . • Security Policy enforcement. • Management Support.
Protect Against Unintentional Insider Threats: The risk of an employee's cyber misconduct on a Social Media Site (Mazzarol et al,	Literature review	- Organizations will certainly depend more on online services like the Cloud in the future. - The unintentional players will not be aware of the fact that they are doing	• Skills and experience of employees. • Ignorance and negligence. • Apathy. • Security Policy

2021).		something wrong; however, they will have unintentionally caused harm to the organization's assets by leaking data or giving access to external cybercriminals. - 80% of the incidents are due to unintentional actions associated with conscientiousness.	enforcement. • Management Support.
(A Multi-Tiered Framework for Insider Threat Prevention Alsowail & Al-Shehari, 2021).	Real-world cases and relevant literature.	- Insider threats are still a major cause for concern for both public and private organizations.	• Budget of organization. • Culture. • Communication. • Security policy enforcement. • Management support. • Situation awareness. • Ignorance and negligence • Skills and experience of employees.

2.7 Unintentional Insider Threats Issue in Malaysia

Insider threat and the risks related to it is not a new concept for Malaysian organizations. However, majority of these companies are not willing to openly face the risk and instead, wish to deal with it in a subtle manner. These companies are hesitant in sharing their experience and the challenges they faced handling the issues associated with insider threats. This was possibly because of adverse reputation and fear of exposing the fact that trusted individuals from within the organization had been involved in wrongdoings or fraudulent activities and believing that it would have undesirable consequences on the company's functions and customers' views. Insider attacks may damage the reputation of the affected organization (Apau et al., 2018).

Cyber Security Malaysia and Cyber999 in Malaysia documented references, which showed that the percentage increased significantly by 2011. It was found that 87% of all web traffic in Malaysia was malware in February, 2010. The cases increased from 3564 to 8090 from 2009 to 2010. In 2011, a total of 14157 cybercrime

cases were reported. This clearly proves that there has been an alarming increase in cybercrimes. Robin Hicks reviewed the problem of cyber security and shocked the audience of Malaysian civil servants by showing a slide show in which the Malaysian government's website had been hacked and was filled with pictures of naked women. Cybersecurity Malaysia established the Cyber Early Warning System that has identified more than 5,000,000 security threats till August 2012 (Isnin & Sedek, 2018).

It has been deduced in the review carried out on insider threat status in Malaysian organizations that there are two kinds of attackers. The first type is intentional misused, which means that they have become an attacker because they want to negatively affect the organization. The other kinds of attackers are unintentional attackers, where attacks occur due to human errors or mistakes, for example, by accidentally leaking sensitive information about the company over social networks (Tuor et al., 2017, Isnin & Sedek, 2018).

The security threat issues in Malaysian public service organizations were examined by Tarmidi et al. (2013). After performing an extensive analysis 19 computerized accounting threats mentioned in the survey question, the study found that the source of most CAS security threats is internal, i.e., "employees".

It was shown in a few studies, like Waluyan et al (2010), Asai & Waluyan (2008) and Asai & Hakizabera (2010) that international organizations experienced difficulties in implementing Information Security management in Malaysia, Indonesia and East Africa, respectively. This is because the cultural distinctions can pose challenges that influence how the organization deals with the insider threat. The findings showed that there was a strong tendency to share information, which was considered as being natural by the employees and which went beyond the policy

conditions. The study results showed that this was because the employees in the country come from a “highly collectivist society” (Asai & Hakizabera, 2010).

Human-related challenges in information security were experienced by the organizations of investor countries, including the British, American and Japanese. The difference in cultures were examined through surveys in investee countries, i.e., Indonesia, Malaysia, Thailand, India and China and in the Eastern African Community including Brazil, Venezuela and Russia. The data was analyzed and the results showed that United States exhibits the greatest severity in 11 out of the 25 issues analyzed. Malaysia exhibited the greatest severity in the cultural dimensions. Therefore, they need to give greater attention to the issue of unintentional sharing of confidential information (Asai & Perez, 2012).

It was demonstrated by the results regarding the level of likelihood of threats in the computerized banking systems in Malaysia that the human unintentional threats were the most severe issue in terms of the key threats challenging this sector in Malaysia. This was followed by human intentional threats, technological threats, threats regarding the environment, and finally, nattural threats (Malami et al., 2012). Cybercrimes in Malaysia, in particular, have increased by 10,000 cases per year, on average, most of which are online scams and hacking organizational information systems. A total of 1,714 cases of cyber hacking were reported in Malaysia in 2015; however, 1,705 cases were reported in the first half of 2017. This shows that the threat of cybercrimes is increasing in Malaysia, and local organizations would be at a greater risk in the future. There would also be more incidents of insider threats due to rogue users, hijacked systems or accidental user errors. The attacks are increasingly occurring to achieve financial benefits by means of data theft or data leakage. Attackers can share the personal and sensitive information about users on the social

media, and since personal information is easily accessible, the attacks can exploit this information for malicious gains. Attackers can also gain insights from daily routines like responding to emails, texting on WhatsApp, transferring files on the USB, etc., and exploit this information. With the easy accessibility of different types of data, including confidential data, miscreants can determine passwords, pins and sensitive information and misuse them. The attackers can spread malware through infected programs, email attachments and hacked websites. They restrict the victim from accessing their computer system, files or mobile device till they have paid a ransom. However, even after making payment, it is not guaranteed that they will successfully get access to encrypted files or device/computer storage (Abas, 2017).

Table 2. 4: Summary of studies and surveys on UITs in Malaysia (2010-2021)

Author	Key findings
(Asai, & Waluyan, 2008)	The findings demonstrate a strong inclination towards exchanging information.
(Waluyan et al, 2009).	UITs are the most significant security threats faced by Malaysian organizations.
(Roy, 2010).	Over 10,000 reports and cases are received by cybersecurity Malaysia with respect to cyberattacks and crimes each year. The main issues emerge from humans themselves.
(Samy et al., 2010)	A significant internal threat faced when implementing Health Information System in Malaysia is human error.
(Asai & Perez,2012)	UITs are the greatest security threats experienced by Malaysian companies.
(Humaidi & Balakrishnan, 2013).	One of the key internal threats faced in the implementation of Health Information System in Malaysia is human error.
(Amiruddin, 2016).	Malaysia exhibits the greatest vulnerability to cyberattacks. Malaysia is considered as one of the top ten countries at risk of cyberattacks. The risk of cybercrimes is experienced by 65% of Malaysian organizations.
(Tuor et al.,2017	Unintentional attacks were faced most commonly
(Isnin & Sedek,2018)	Unintentional attacks were faced most commonly
(Khalid,2020; Samy et al., 2021)	Losses of 1 billion RM were faced by the Malaysian cyber-criminal, which made the country the fifth most risky country to cyber threats in 2013. The key challenges presented by individuals in the enforcement of cyber security in Malaysian public sector firms were inadequate skills in the staff, lack of liability in terms of cybersecurity and human error.
(The Global State of	It is expected that there will be a continuous increase in cybercrimes

Information Security, 2020)	and information security threats in Malaysia, and this issue will become a major cause for concern for public security and the country's economy. This will present serious threats if no attempts are made to decrease or avoid them. It was reported in 2017 that WannaCry affected over 150 countries all over the world, including Malaysia, with almost 200,000 cases, with the overall number of actual attacks not clear. The Malaysian computer emergency response team (MyCERT), which is a cybersecurity department in Malaysia, reported in 2019 that Malaysia experienced more than 400 defacement incidents by 31st August 2019 that involved 19 government organizations. Though efforts have been made by the Malaysian government through different organizations to avoid cybercrimes and information security threats by enacting various cyber laws and policies, controlling such threats depends on the people. Merely 11% of the revenue earned by organizations is spent on security defences that particular aim to decrease insider threat.
(Shammugam et al.,2021)	The findings of this study showed that technical challenges, spyware, bluesnarfing threats, phishing, social engineering and virus, malware, trojan, ransomware, viral websites threats are the main types of threats that the Malaysian public sector organizations frequently face. These threats are faced due to insufficient budget, skilled personnel, and workforce for security tasks, user awareness; lack of conformance and monitoring, and inadequate security policies and regulations.
(Ulven & Wangen,2021)	The key threat agents prevalent in higher education included malware, intrusion and other kinds of compromises, risk assets and scanning, unintentional disclosures, organized crime, social engineering attacks, state-supported espionage and human errors. The threat gates include inadequate information security knowledge and awareness, or a lack of best-practice security controls.
(ASEAN cyber threat assessment,2021)	There are no signs of phishing attacks in the ASEAN region slowing down or ending. Kaspersky alone blocked and prevented over 1.6 million attempts to phishing against SMBs in Malaysia, Indonesia and Vietnam in the first half of 2010. The data by Kaspersky demonstrates that 442,439 cases occurred in Malaysia. There was a 60.5% increase in the number of cases. On the whole, 7,765 cases were registered with CyberSecurity Malaysia by August, 2020. Fraud was at the top of the list with 5,697 cases registered in comparison to 4,671 cases for the same time frame in 2019. Malaysia experienced an increase in scam cases between January and October 2020, with a total of 5,218 cases. This signified a loss of more than 256 million Malaysian Ringgits (MYR). The past few years has seen a rapid growth in the average rate of Internet penetration in Southeast Asia, with no signs of slowing down. There is an 83% internet penetration rate in Malaysia.

The importance of the literature review on the UITs issue in Malaysia, which was conducted in this research, appears, in that it highlights on these threats and raises the alarm to take them into account and not to underestimate them.

2.8 Existing Countermeasure of UIT

Different strategies to handle human error were presented by various authors. The models and countermeasures that were identified from a literature review in this field of study are discussed below.

2.8.1 Automation

Automation refers to the deployment of information technologies to take decisions for the user. For example, automated functions within a computer could be increased by making a popup menu appear on an employee's computer screen that notifies them to change their password. In addition, coping skills could be included in an IT system. As there are several security failures that are related to humans, it may be better to employ techniques with very little human involvement. The greater predictability and precision of automation compared to humans is its strength. The old anti-virus program that required system users to determine whether to quarantine, clean or ignore a detected virus is an example of automation. In the latest versions of the anti-virus programs, there is automatic cleaning of the viruses following detection. An important point to note is that it is not possible to automate every end-user system function (Carstens et al, 2004).

Edwards et al. (2007) presented the following directives for automating security

- It should be possible to reverse automation solution.
- The actions of a system should be perceived by the user.

- The system should have the ability to recover from any automation error.
- Automation is appropriate for those systems that are not perfect
- Automation is recommended for situations in which it is not possible for the system user to perform the task. For example, checking of packets by intrusion prevention systems at a speed that the human systems administrator cannot keep up with.

It is indicated by the literature on human error that automation is paradoxical. Technology can be used to address trivial tasks, while humans can address more challenging tasks (Gonzales & Sawicka, 2002). This means that the issue of human error cannot be solved by automation (Rupere et al., 2012). Training is a one of the most effective ways of combating human error in information security. It was determined in the findings of a study carried out by Computer Technology Industry Association (CompTIA) that there is 20% less likelihood of a company being a victim of security attacks if it is able to train even a quarter of its IT employees (Bean, 2004).

2.8.2 Standard Operating Procedure (SOP)

Standard Operating Procedures (SOP) can be introduced to decrease the issues arising from not adhering to procedures. The different steps that people follow to accomplish a task is known as a standard operating procedure. The advantage of SOPs is that they remove the differences in work performance that arise because of the distinct steps followed by users to accomplish the same process (Rupere et al., 2012).

2.8.3 Trust Model

"The Trust model" is another solution that has been presented by Schneier (2004) to human factors in information security, describing it as "representative of the

way an organization determines who it should trust with its assets or parts of its assets". The Trust model gives permission to a limited people to access specific rooms, open particular cabinet files or sign checks. In some extreme situations, further security is provided by dividing responsibilities, for instance, the person in physical possession of checks is not allowed to access the machine for embossing the signatures. A person may be assigned the task of modifying the personnel records, but not the engineering specifications. Human errors can also be minimized by segregating responsibilities. This is because it is assumed that errors can be made by people only in the field in which they are assigned tasks.

2.8.4 Brown's Solutions to Human Error

Four categories were presented by Brown (2004) for dealing with human error. These are error prevention, spatial replications, temporal replication and temporal re-execution. Error prevention is a precautionary approach that aims at preventing human errors from occurring. The rest of the three categories focus on the errors that have already occurred. Using a combination of any of these approaches typically gives rise to systems that minimize human error.

2.8.4.1 Error Avoidance

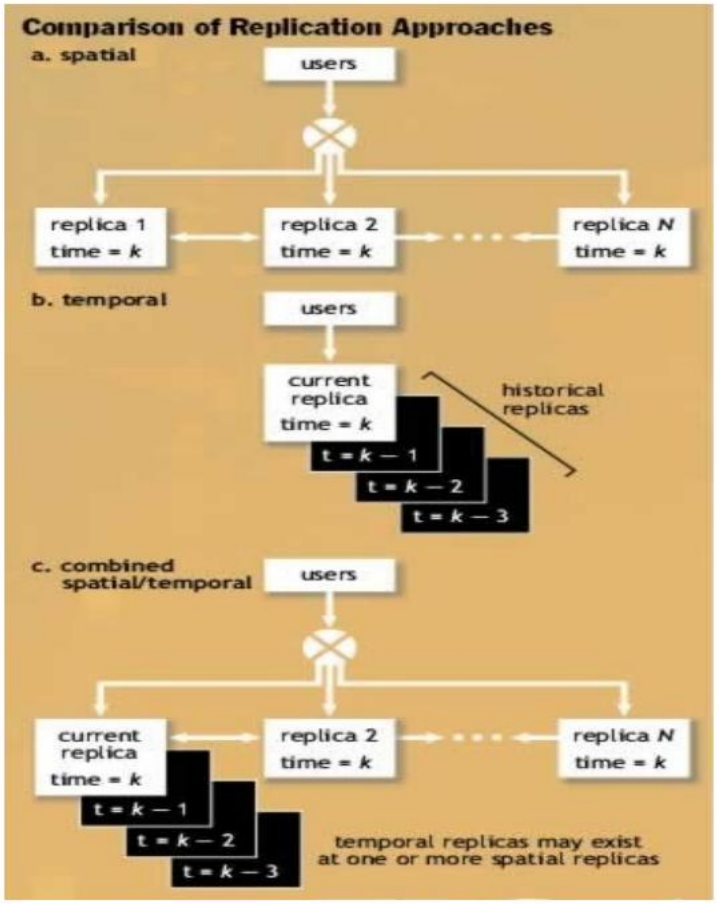
Error avoidance is attained by making sure that the system users do not carry out any errors (error avoidance) along with strategies to avoid the errors from entering into the system (error interception). To achieve error avoidance, the errors should be foreseen before they occur. Error avoidance can traditionally be attained by carrying out continuous training along with a suitable user interface design.

2.8.4.2 Spatial Replication

The strategy addresses errors that have already occurred. The strategy works by creating a large number of copies of a system. Every copy of the system has its own duplicates of the critical information regarding the system that is synchronized. The disadvantage of this approach is that it is only appropriate in cases when human error affects only a few replicas. As a result, errors having an impact on a greater number of the replicas are considered as the appropriate system state.

2.8.4.3 Temporal Replication

The difference between temporal replications and spatial replication is that temporal replications maintain multiple copies of the system, each of which has its own duplicate of the system state. The key distinction is that there is no synchronization between the replicas used in temporal replication. An existing copy of the system is used in temporal replication that shows the actual state of the system, and different replicas (historical) will show the situation of distinct states in the system's history. It is only the present replica that is affected by the requests to the system along with the human operator input. The distinction between spatial and temporal replication is demonstrated in Figure 2.12 overleaf. A significant disadvantage is that this technique is appropriate for cases in which human errors influence the system state. Protection against operational errors that influence the system state can be achieved using a combination of temporal replication and re-execution, referred to as replication with re-execution.

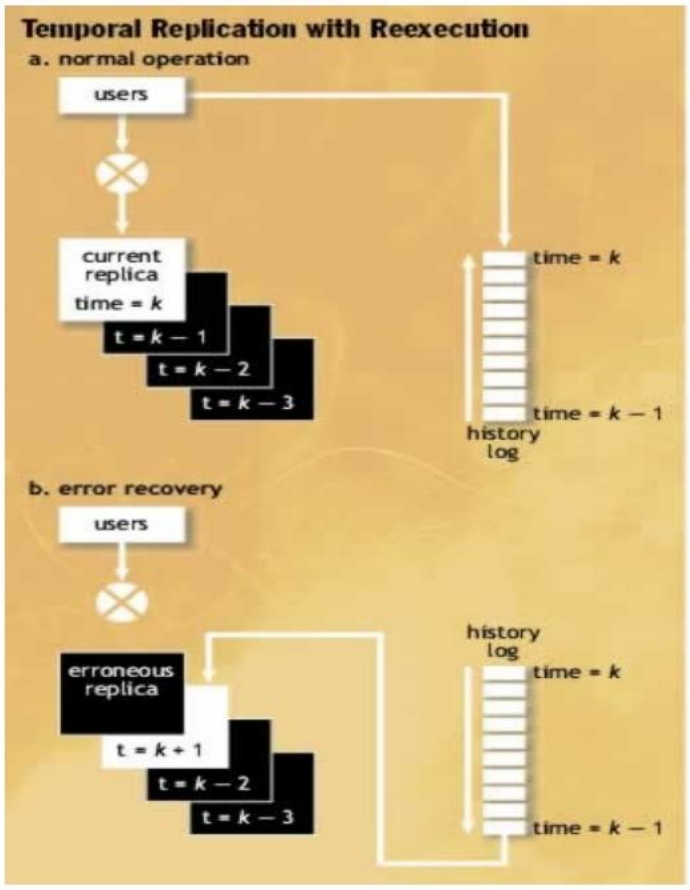


Source: Brown (2004)

Figure 2. 12: Comparison of replication approaches

2.8.4.4 Temporal Replication with Re-execution

A separate history log that includes the different changes that have occurred from the time the last temporal replica was created is employed in this approach. When a human error is made, it is solved by the system by shifting to the old replica and then re-executing the transactions to update the replica. Figure 2.13 overleaf shows this process.



Source: Brown (2004)

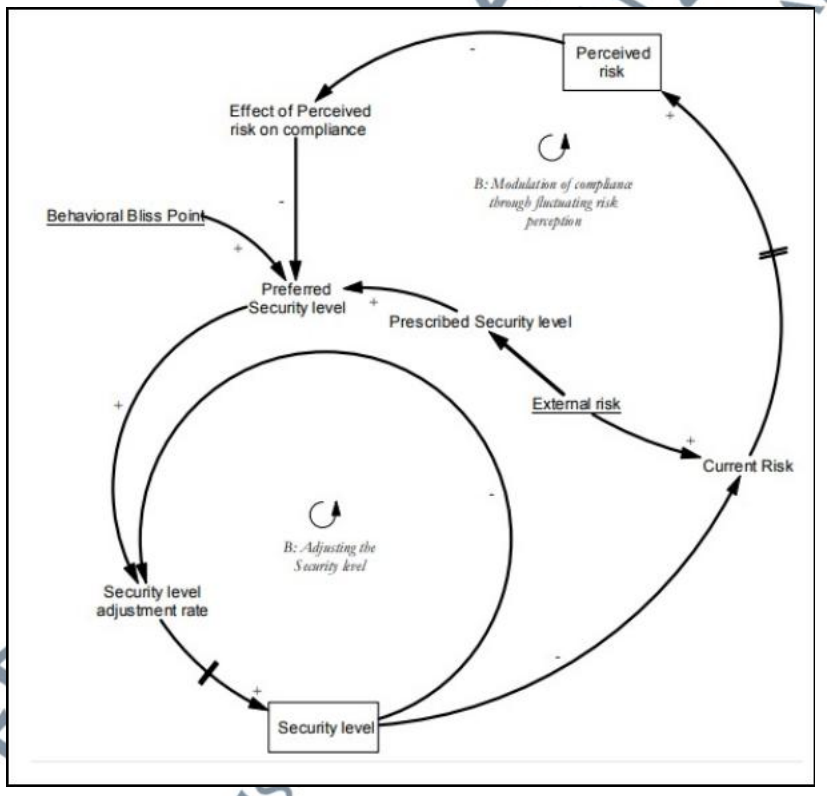
Figure 2. 13: Temporal replication with re-execution

A disadvantage of this approach is that it is very difficult to execute this error-recovery strategy. It is important to be very careful when generating and re-executing the history log to attain the causal ordering of events. When the system is heavily-loaded, it may be expensive to perform re-execution with respect to time and storage requirements.

2.8.5 Framework for Human Factors in Information Security

The issue was considered by Gonzalez & Sawicka (2002) by taking a social sciences perspective. The objective of their study was better comprehended how human factors affected information systems security. The basis of the model was the

behaviour al regulation theory that is explained most appropriately through instrumental conditioning. Instrumental conditioning is defined as learning through consequences. The important aspect of this model is that a subject or user should comply with security practices and also risk perception. Instrumental conditioning is based on the idea that a system user's behaviour that generates positive outcomes is reinforced, while behaviour that generates negative effects is discouraged. An imaginary case was used by the researchers to show that formulating good security policies can be improved by using system dynamics. The overleaf describes the main aspects of the model that is best described using a causal structure diagram.



Source: (Gonzalez & Sawicka, 2002)

Figure 2. 14: Causal loop diagram of security dynamics under the influence of risk perception

The focus of the model presented by Gonzalez & Sawicka (2002) is on conformance to IT policy along with risk perception. The researchers were of the view that conformance to security measures can be affected by factors like throughput pressure. These researchers asserted that alertness to risk can help attain conformance to security policies. This suggests that if a person recognizes a security attack, they can show higher caution and adherence to the IT policy. However, if a person does not sense a security attack, they become relaxed and rarely, or do not, follow the IT policy. It was shown in their model that a user shows higher tendency to follow policy when they have a comparatively higher anticipation of risk. Security attacks tend to increase a user's anticipation of risk. A person's perception to risk increases with the occurrence of security incidents. In contrast, when security attacks are absent, there is a decrease in risk perception. Though security attacks positively influence compliance, it is not the best way of bringing about compliance to policy. Other methods need to be followed to maintain a suitable level of risk perception. There are various shortcomings in this model from this perspective. First, an imaginary case of a person (Kim) is used to explain the key concepts of the model, while proper research samples (multiple individuals) are employed. Second, it is not clear how the samples were chosen, e.g., computer literacy level. Third, the model is quite theoretical and hence, cannot be proven mathematically. These shortcomings in the model by Gonzales & Sawicka (2002) make it imperative to generate a new model.

2.8.6 A Generic Model of Human Factor Management

Trcˇek & Kandus (2003) presented this model and the key issues in this model are the real risks (RR) and perceived risks (PR). The rate of adaptation, which refers to a change in perceived risk (CPR) and accumulates as PR, is directly related to the

difference between real risk and perceived risk, and inversely related to real adjustment time (RAT). It is deduced that PR is a level determined by CPR. There are two elements that show that RAT is determined by a few circumstances. These are the initial one and a contribution of experiences. For example, following a long period of a lack of accidents, when an accident occurs, the expectations are based on earlier experiences. This means that the users consider this accident as a rare event. On the contrary, if attacks are experienced consistently for a long time, people will expect a similar attack to occur any time in the future. This fact is stressed in the model by incorporating length of normal operation (LNO) variable. The level of security policy also affects the change in perceived risk – the greater the level, the higher the rate of adaptation. A change in security policy level (SPL) occurs with a delay because RR is always ahead of reported risk, which is also true for discrepancy and internal accidents frequency (IAF). The fundamental notion of the model is that individuals should avoid violations and real risks should be adequately perceived, that is in a timely manner and in regards to the number of threats. The following figure (Figure 2.15) shows the model.

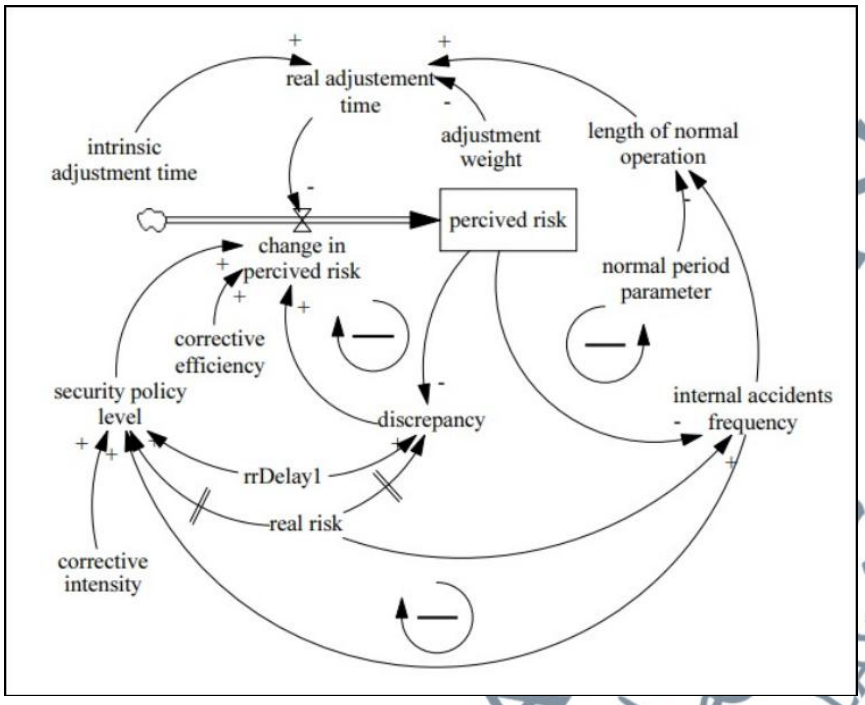


Figure 2. 15: A generic model of human factor management for security policy

The fact that RAT depends on some specific situations is shown by a contribution from experiences. For example, if a person has been inflicted with serial attacks for a long time, he/she will always be wary of the next attack. This person becomes more careful and vigilant regarding the security measures. In contrast, if a person does not experience an attack for a long time, they become relaxed and may not adhere to any security practice. The level of security policy also determines the change in perceived risk, i.e., the greater this level, the higher the rate of adaptation. There are three balancing loops in the system. The upper left loop refers to the loop of perceived risk (PR, RPR, CPR, discrepancy). The trust loop in the upper right corner represents the trust of employees in the system, keeping in view the standard operations experiences, which affect RAT. The adjustment loop is at the bottom, which shows the adjustment of anticipated risk that is a result of the management through SPL. Like the earlier model, i.e., the framework for human factors in information security by Gonzalez & Sawicka (2002), this model does not include

various significant issues. Firstly, the model is quite narrative and does not exhibit scientific soundness. Second, it does not employ particular variables of information security, for example insider attacks, social engineering, etc. Finally, the model is too theoretical and cannot be proven mathematically (Rupere et al., 2012).

2.8.7 Collaborative Reinforcement Model

A reinforcement framework was presented that allows for collective monitoring of policy violations by system users. A rewards model was presented to execute the framework. Suitable reward, punishment and also community price were defined in the model, based on reporting an actual or false violation. In addition, the model also considered non-reporting of the breaches identified, along with previous reporting of vulnerabilities by the users. The model is based on the idea that the users should be made responsible for information security by making them actively involved in various aspects of security, for example in perceiving threat and monitoring policy breaches. An example of the Reinforcement model for collaborative security works presented by Saha & Misra (2009) is better monitoring and reporting of a malicious user carrying out destabilizing modifications in a code base by the relevant team members, who are likely to have better knowledge of it or can better identify it compared to the centrally administered monitoring systems (Saha & Misra, 2009).

The following assumptions are part of the human error model presented by Saha and Misra:

1) It is believed that a violation has an observable effect to remove cases of false reports deceptively.
2) An IT policy that is strictly followed is displayed in every organization.

3) A violation is recognized only after there are reports of its occurrence. Other users or monitoring equipment achieve the detection. This means that if a violation occurs but none of the witnesses report it (or it is not captured by the monitoring device), it would be considered as not detected.
4) Users have access to security policies and can detect and report actual violations.

The model was justified by various social psychological studies that considered the part played by extrinsic motivation in affecting individual and group behaviour s. The conclusions of a few of these studies are listed below:

- Group punishment helps in achieving extended community behaviour s. Individuals in groups are capable of affecting others so that they can avert collective punishments caused by other group members.
- Extrinsic rewards can drive new (community) behaviour s.
- Punishments, along with rewards, also serve as negative reinforcement strategies for individuals attempting to avoid punishments. However, individuals may revert to their past habits if they do not internalize anticipated behaviour s.
- It is demonstrated by sociological studies that focus on the locus of control that there is higher motivation in individuals when they believe that they have greater control over their environment. Users are typically allowed by collaborative security to help in policy design. When they are able to monitor their violations, they acquire a sense of control over the assets and policies they are using compared to those situations in which they make little or no contribution to these aspects. Various researchers have adopted the approach of using reinforcement to attain information security. Saha & Misra (2009)

who presented the Reinforcement Model for Collaborative Security also stressed that when developing security policies, a socio-psychological understanding of individual and group behaviour should be used. The authors stressed on the need to formulate policies and environments that give rewards to employees for reporting security breaches.

To sum up, the model is based on the key idea that users work alongside each other to make sure that every organizational member follows information security policy. Individuals are then rewarded and punished on the basis of their actions.

2.8.8 Generic Mitigation Strategies for Information Leaks (2019)

For unintentional insider threats, (Ismail & Yusof, 2019) developed the security tool in four domains containing the generic mitigation strategies, namely: organization, technology, people and processes, which have further sub-components, such as: Prevention and Detection, Investigation, Culture, Description, Managerial, Behaviour, Job process and Physiological. There are different elements in sub-components, for instance, technologies for error monitoring, interception, detection and solutions. Besides the top management must take the following factors into account, such as: enforcement of system security policies, standards, baseline, laws, procedure, security and regulation, monitoring and control of the job process, educational training awareness, data classification, data flow, job rotation, access control, the working environment and organizational culture.

The relationships among the sub-element groups of the tool were suggested by this security tool. There is a connection between each sub-element groups in the security control and each element complements each other. These relations between the sub-element groups are represented by the dotted line. In the security control, the

relationship between risk analysis and security metrics processes is represented by the dashed line. The relationship between monitoring and auditing processes to the sub-groups in the security is demonstrated through the dash-dotted line. Figure 2.16 depicts the security tool developed by (Ismail & Yusof, 2019).

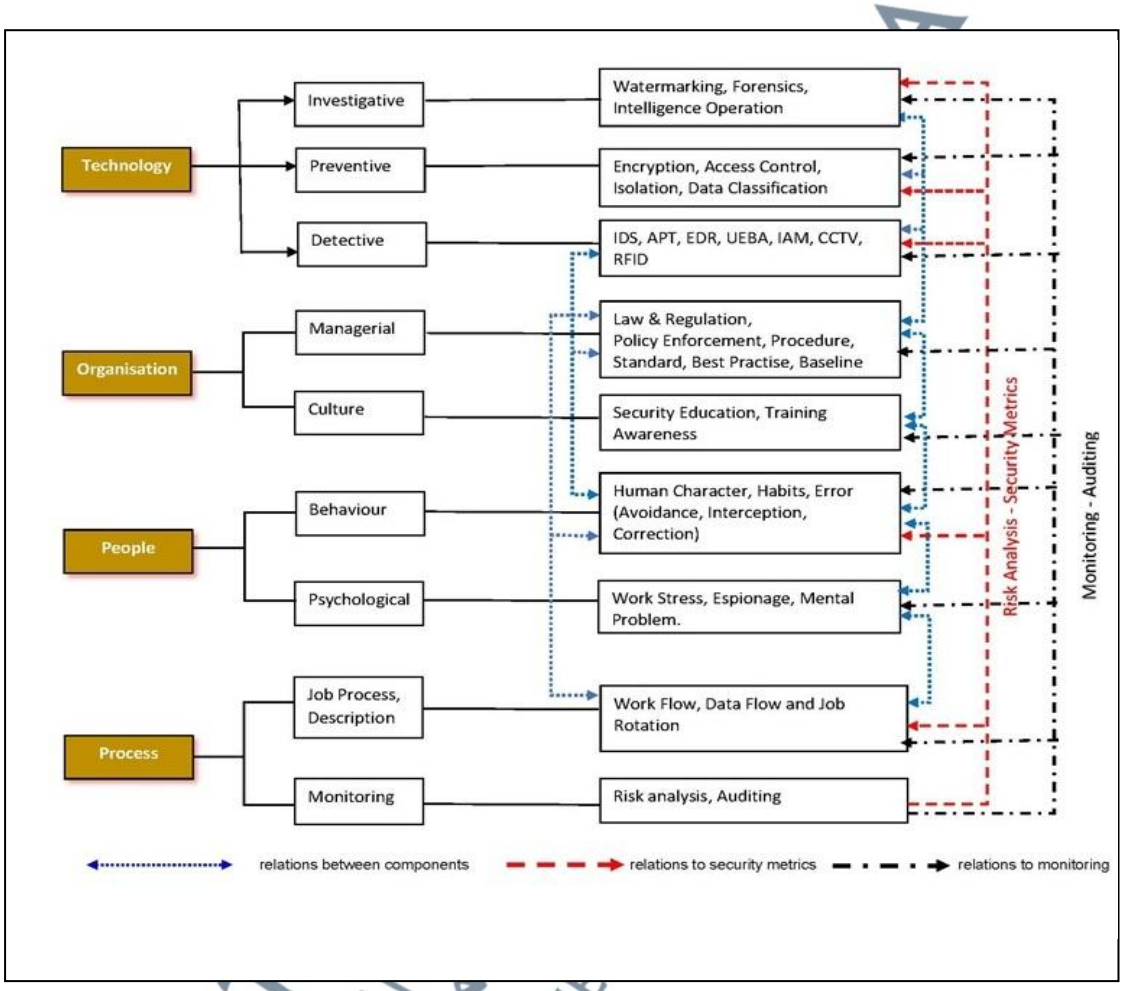


Figure 2. 16: Generic Mitigation Strategies for Information Leaks (2019)

2.8.9 UIT Mitigation Strategies and Countermeasures (Greitzer et al, 2014)

A work project was built by (Greitzer et al., 2014). The UIT cases were acquired in the CERT insider threat database and discovered in public sources and based on the reports. The study findings presented various countermeasures of UIT that are presented in the following Table and are referred to as UIT Mitigation Strategies and Countermeasures by Greitzer et al. (2014).

Table 2. 5: UIT Mitigation Strategies and Countermeasures by (Greitzer et al., 2014)

Human Factors and Training	High-Level Organizational Best Practices	Automated Defence
* Improve awareness regarding insider threat and UIT. * Increase motivation to be cautious with respect to UIT risks. * Provide training to employees so that they can detect phishing and other social media threat vectors. * Stimulate process discipline to bring about adherence to policies and guidelines. * Perform continuous training to ensure adequate level of skills, knowledge and ability. * Carry out training and enhance awareness of risk perception and cognitive biases that have an impact on decision-making. * Increase usability of security devices. *Increase usability of software to decrease the possibility of system-induced human errors	* Evaluate and enhance management practices to make sure resources are aligned with tasks. * Enhance data flow by improving communication and ensuring accurate procedures. * Decrease distractions to ensure productive work environment. * Offer effective security measures (e.g. two-factor authentication to gain access). * Carry out effective work planning and regulation to decrease job pressure and manage time. * Maintain employee enthusiasm * Uphold staff values and attitudes that are consistent with organizational vision and ethics. * Adopt security best practices all through the organization.	* Use better software to identify fake emails. * Use data loss prevention software to identify possibly malicious sites and email practices. * Install firewalls. * Deploy virus and malware protection software. * Enable remote memory wipe for lost equipment.

2.9 Limitation of Existing Countermeasure

To list the countermeasures of UITs in place, a literature review was carried out. These countermeasures were then evaluated to identify the strengths and weaknesses of each. The advantages and disadvantages of the prevailing countermeasures of the human error elaborated in section 2.8 are presented in Table 2.6.

Table 2. 6: Advantages and Disadvantages of the Existing Countermeasures of the Human Error

Strategy	Advantages	Drawbacks
Automation.	1. Automation is more predictable and accurate that its' human counterparts. 2. Since many security failures are attributed to humans, then it could be wise to use techniques that involve minimum human intervention. 3. Automation is highly commendable in cases where it is absolutely impossible for the system user to do the work. An example is where packets are checked by intrusion prevention systems at a speed that exceeds that of a	1. Automation can addresse only trivial tasks leaving more demanding tasks to people (Gonzales & Sawicka 2002). This implies automation is not going to be the solution to the human error problem, but something else (Rupere et al, 2012).

	human systems administrator.	
Standard Operating Procedure (SOP)	1. SOP eliminates the differences in work performance that are as a result of different steps followed by users to complete the same process (Rupere et al, 2012).	1. SOP addresses only the differences in work performance it is very limted. It does not solve the other problems related to technological, organizational and human factors aspects.
Trust model	1. The Trust model reduces the chances of errors occurrence by given permission to only certain people to certain tasks such as, given permission to certain rooms, open certain cabinet files, or sign cheques.	1. The Trust model reduces only the chances of errors that related to certain people it is very limited. It does not solve the other problems related to technological, organizational and human factors aspects.
Brown's solutions to human error.	- Brown proposes four solutions for human error:- 1. Error avoidance by ensuring that system users do not commit errors by use of continuous training in collaboration with good user interface design as well as strategies to prevent the errors from penetrating the system (error interception). 2. Spatial replication: is the creation of several copies of the system's important information. These replicas are synchronized. 3. Temporal replication: is the creation of several copies of a state of the system.These replicas are not synchronized. Each one of the replicas represents the situation of different states in the system's history. Human operator input affectes only on the current replica. 4. Temporal replication with Re-execution: uses a separate history log that contains a series of all changes from the time the last temporal replica was made. In the event that a human error occurs, the system solves it by switching to the old replica and then re-executes the transactions in the log, so that the replica becomes up to date.	1.Error avoidance: In order to accomplish error avoidance, it is should be possible for the errors to be anticipated prior to them occurring. 2.Spatial replication : It is most suitable in cases when only the minority of the replicas is affected by human error. Consequently errors affecting the greater proportion of the replicas are accepted as the correct state of system. 3. Temporal replication: Works well for cases whereby human errors affect only the system state. 4.Temporal replication with re-execution It is the most difficult error-recovery strategy to implement. Great care has to be taken when creating and re-executing the history log so that the causal ordering of events is achieved. If the system is heavily-loaded re-execution can be expensive in terms of time and storage requirements.
Framework for Human Factors in Information Security (Gonzalez & Sawicka ,2002)	1. The main idea of instrumental conditioning is learning through consequences, means that a system user's behaviour that produces positive results is reinforced while behaviour that produces negative effects is weakened (reward andpunishment policy).	1. According to (Rupere et al., 2012) the authers used an imaginary case to demonstrate that designing good security policies can be enhanced by use of system dynamics. 2. According to (Rupere et al., 2012) the model cannot be mathematically proven, it is too theoretical.
A Generic Model of Human Factor Management (Trcˇek & Kandus,2003)	1. The basic idea of the model is that user should not violate breaches, if real risk is properly perceived, that is on time and in terms of number of threats. If user experiences serial accidents, for	1. According to (Rupere et al., 2012) the model is too narrative and lacks scientific soundness. 2. According to (Rupere et al., 2012) It does not use specific

	a long time, he / she will be anticipating the next accident. Consequently such a user becomes more careful and is cautious with the security measures. On the other hand, if user experiences long periods of time without accidents, user tends to relax and may not practice any security strategies. The higher contribution from experiences, the faster the rate of adaptation (risk perception). 2. The central issues in the model are: Real risks and perceived risks. The rate of adaptation, that is, change in perceived risk, which is accumulated as perceived risks, is proportional to discrepancy between real risk and perceived risk, and inversely proportional to real adjustment time. It follows that perceived risks is a level, driven by change in perceived risk.	variables of information security such as social engineering, insider attacks etc. 1- 3. According to (Rupere et al., 2012) the model cannot be mathematically proven, it is too theoretical.
Collaborative Reinforcement Model Saha & Misra (2009)	1. In this model, system user's work collaboratively to ensure that information security policy is adhered to by every member in the group the model enables collective monitoring of policy breaches by system users who can better detect violation than the centrally administered monitoring mechanisms. Non-reporting of detected violations, together with prior reporting of vulnerabilities by the users was also considered. Certain rewards and punishments are then awarded to individuals, depending on their actions. The probability of a policy violation being reported is then calculated using specific mathematical formula.	1. If a member of a group has strong personal relationships with other group members, one may not report a violation, in attempt to protect good reputation and for fear of isolation. 2. Determining the actual is a major challenge since individuals vary in their choices of preferred rewards. One may be motivated by special recognition while another may be motivated money. 3. The need for establishing adequate regulations and controls aimed at preserving the privacy of group members.
(Generic Mitigation Strategies for Information Leaks) (Ismail & Yusof, 2019)	1. The security tool presented many of mitigation strategies for UITs in four domains, technology, organization, people and processes. 2. It is considered generic and has enough flexibility to allow for planning for expandability by adding more countermeasures in each domain separately.	1. The security tool misses out many of important aspects, such as design of work environment, design of user-system interfaces, instrumental conditioning, trust model, stimulation of risk perception, incident-driven reviews to policies, practices and training materials and periodically, fully re-evaluate risk.
UIT Mitigation Strategies and Countermeasures (Greitzer, et al,2014)	1. The UIT Mitigation strategies presented many of countermeasures against UITs in three domains; human training, best practices and automated defence.	1.The UIT Mitigation strategies misses out many of important aspects, such as design of work environment, design of user-system interfaces, instrumental conditioning, trust model, stimulation of risk perception, incident-driven reviews to policies, practices and training materials and periodically, fully re-evaluate risk .

The review of existing countermeasure of UITs showed that, the existing countermeasures are insufficient; defending unintentional insider threats requires implementing multi layered defensive approaches including policies, procedures ,technical controls , awareness , attention to sociology , psychology aspects and automated defence tools in at all stages of the incident. Which are prevent, detect and respond stage. Each one of the existing countermeasures that discussed above address an aspect or some aspects of human errors. None of them have does not fully cover all countermeasures in all aspects, technological, organizational and human factors aspects. According to the literature, (Rupere et al, 2012) criticized Brown's solutions to human error, because it's required should be possible for the errors to be anticipated prior to them occurring. (SOP) and trust model does not include the technological, organizational and human factors aspects. Gonzalez and Sawicka framework and Trcˇek and Kandus model, are too theoretical and cannot be mathematically proven.

Model of Saha and Misra does not determine exactly the security issues which they study (Rupere et al, 2012). According to (Gonzales & Sawicka 2002), the problem of human error will not solve by automation. While UIT Mitigation Strategies by (Wan, 2019) and UIT Mitigation Strategies by (Greitzer et al., 2014), were the most comprehensive and more covering to the problem aspects, but they miss out some important aspects, such as design of work environment, design of user-system interfaces, instrumental conditioning, trust model, stimulation of risk perception, incident-driven reviews to policies, practices and training materials and periodically, fully re-evaluate risk. This is the reason why this research project sought to develop a conceptual framework via combining the existing models and countermeasures and identified in the literatures. Therefore, UITCM model can be

used by decision makers to develop training program and as guidelines to support an organization's countermeasures against UITs.

2.10 Unintentional Insider Threats Countermeasure Model in SMEs

Based on the literature review, it was found that there is a need to develop a new model that includes all the existing countermeasures and combine them with each other. Therefore, this study developed the initial version of UITCM by integrating the countermeasures found in the literature, which were listed and compared in this chapter, so that it provides a comprehensive approach to mitigate unintentional insider threats. To develop the second version of UITCM, a survey was conducted towards IT Executives of Malaysian SMEs, to identify factors and likelihood of UITs in Malaysian SMEs. This study identified the likelihood of UITs to justify the need for the proposed model and examined whether the study problem still existed by identifying the likelihood of UITs. The most contributing factors of UITs have been identified in order to give them more focus and concern during the model development process and to ensure that they covered from all its aspects. The questionnaire of this study serves as a roadmap for developing the second version of UITCM by determining of how much the need for the model, as well as identifying the most contributing factors of UITs to be fully covered. Then the study compared the solutions provided by the new model with the contributing factors of UITs to prove that the proposed model covered all possible solutions to these threats.

2.11 Component Investigation

A model should be checked before usage, in order to validate that the theories and assumptions underlying the model components still hold (Elmimary, 2017). The

justification conducted in this section ensures that the construction, reason and fundamental relationships and the illustration of the problem area are sufficient for planned purpose. As of this research, the model investigation determines that an agreement is achieved between the components introduced in the new model and those that existed in the base models. The investigation of the proposed model presumes that the model should be refined and improved. It is important to ensure that the new developed model included and covered components of the selected UITs mitigation strategies and countermeasures recommended in the literature. To achieve this components investigation, a critical step- by- step comparison was conducted between the proposed model and the existing models which were used to develop the proposed model to ensure that the new model covered all components of the existing models.

In order to conduct this investigation, the components of the second version of UITCM are listed with unique identity (ID) in Table 2.7, Table 2.8, and Table 2.9 and the selected UITs mitigation strategies and countermeasures recommended in the literature are assigned with unique identity (ID) as depicted in Table 2.7. Once the components of the (UITCM) and existing mitigation strategies are listed with their 'ids', the next step is to compare the components of each one of the existing mitigation strategies with the components of the second version of UITCM. The result is displayed in Tables 2.8, 2.9, 2.10 and 2.11

Table 2. 7: The Organizational Countermeasures Components

Components of the Second Version of UITCM	
ID	**The Organizational Countermeasures Components**
OC01	-Law &Regulation, Policy Enforcement, Procedure, Standard, Best Practice, Baseline, Standard Operating Procedure (SOP).
OC02	-Maintain employee readiness.

OC03	- Improve data flow.
OC04	- Effective security practices.
OC05	- Maintain staff values.
OC06	- Improve design of user-system interfaces.
OC07	- Affordable access to mental health/drug treatment services.
OC08	- Appropriate time off for employees.
OC9	- Team-building activities to enhance mood.
OC10	- Improve design of work environment.
OC11	- Improve work planning and control.
OC12	-Improve work setting and management practices.
OC13	- Risk analysis, auditing.
OC14	-Incident-driven reviews (policies, practices, training materials).
OC15	- Periodically, fully re-evaluate risk.

Table 2. 8: The Human Factor's Countermeasures Components

Components of the Second Version of UITCM	
ID	**The Human Factor's Countermeasures Components**
HC01	-Monitor employee behaviour.
HC02	-Trust model.
HC03	- Collaborative Reinforcement Model.
HC04	-Mental problems test.
HC05	-Drug testing.
HC06	- Stimulation of risk perception.
HC07	-Security education, Training, awareness, Instrumental conditioning.
HC08	-Usability of software /security tools.
HC09	-Encourage following of policies.
HC10	-Employee assistance programs (EAPs).
HC11	-Respectful and calm workplace environments.

Table 2. 9: The Automated Defence Tools Countermeasures Components

Components of the Second Version of UITCM	
ID	**The Automated Defence Tools Countermeasures Components**
AC01	- Watermarking forensic, intelligence operation.
AC02	-Backup systems (Spatial /Temporal) Replication.
AC03	- Remote memory wipe for lost equipment.
AC04	-Automation.
AC05	-Data encryption/Password protection.
AC06	-Wireless and Bluetooth safeguards.
AC07	- Standard systems/email safeguards (anti-phishing, anti-malware etc), prevention system (IDS/IPS,DLP), firewalls, APT prevention, accesses control, static and dynamic software code checkers, data classification, IAM.
AC08	-Security information event management (SIEM) systems, software to recognize bogus emails, EDR, UEBA, CCTV, RFID.

Table 2. 10: The Selected UIT Mitigation Strategies and Countermeasures Recommended

ID	Year	Mitigation Strategies Name
C01	2019	Generic Mitigation Strategies for Information Leaks(Wan,2019)
C02	2014	UIT Mitigation Strategies and Countermeasures (Greitzer et.al, 2014)
C03	2002-2012	Suggested solutions in the literature: -Automation (Carstens et.al, 2004; Edwards et.al, 2007; Gonzales & Sawicka 2002; Rupere et al, 2012). -Trust Model (Schneier, 2004). -Standard Operating Procedure (Rupere et al, 2012). -Brown's Solutions to Human Error (2004). -Framework for Human Factors in Information Security (Gonzalez & Sawicka, 2002). -A Generic Model of Human Factor Management proposed by (Trcˇek & Kandus, 2003). - Collaborative Reinforcement Model (Saha & Misra, 2009).
C04	1986-2013	Recommendations of studies (HSE,1999;Wood & Banks, 1993;Bratus et.al, 2008;Kerm et al,2007;Jeffrey et al,2002;Mansor et.al, 2011;Murphy et.al, 1986;CERT,2013).

As a result of the components and processes validation technique, the components of C01, C02, C03 and C04 were compared against the components of UITCM. The UITCM was revised many times and adding the missing components which have not been covered by the previous version or removing the duplicate components to ensure that the proposed UITCM includes all necessary mitigations chosen to complete the model.

Table 2. 11: C01 Against the Second Version of UITCM

C01 Components	UITCM Components
- Watermarking forensic, intelligence operation.	AC01
-Encryption, accesses control, isolation, data classification	AC05, AC07,
- IDS, APT, EDR, UEBA, IAM, CCTV, RFID	AC07, AC08
-Law &regulation, policy enforcement, Procedure, standard, best practise, baseline.	OC01
-Security education, training awareness.	HC07
-Human character, Habits, Error (Avoidance, Interception, correction).	OC01, OC02, OC03, OC04, OC05, OC06, OC07, OC08, OC09, OC10, OC11, OC12, OC13, OC14, OC15, HC01, HC02, HC03, HC04, HC05, HC06, HC07, HC08, HC09, HC10, HC11, AC01, AC02, AC03, AC04, AC05, AC06, AC07, AC08,
-Work stress, espionage, mental problems.	OC07, OC08, OC11, HC04,HC05
-Work flow, Data flow, job rotation.	OC03, OC11, OC12
-Risk analysis, Auditing.	OC13

Table 2. 12: C02 Against the Second Version of UITCM

C02 Components	UITCM Components
-Enhance awareness of insider threat and UIT.	HC07
-Heighten motivation to be wary of UIT risks.	HC07, HC06

-Train employees to recognize phishing and other social media threat vectors.	HC07
-Engender process discipline to encourage following of policies and guidelines.	HC09
-Train continuously to maintain proper level of knowledge, skills, and ability.	HC07
-Conduct training on and improve awareness of risk perception and cognitive biases that affect decision making.	HC07, HC06
-Improve usability of security tools.	HC08
-Improve usability of software to reduce likelihood of system induced human error.	HC08
-Review and improve management practices to align resources with tasks.	OC14
-Improve data flow by enhancing communication and maintaining accurate procedures.	OC03
-Maintain productive work setting by minimizing distractions.	OC12
-Provide effective security practices (e.g., two factor authentication for access).	OC04
-Implement effective work planning and control to reduce job pressure and manage time.	OC11
-Maintain employee readiness.	OC02
-Maintain staff values and attitudes that align with organizational mission and ethics.	OC05
-Implement security best practices throughout the organization.	OC12
-Deploy better software to recognize bogus emails.	AC07
-Deploy data loss prevention software to recognize potentially harmful sites and email practices.	AC07
-Use firewalls.	AC07
-Use virus and malware protection software.	AC07
-Enable remote memory wipe for lost equipment.	AC03

Table 2. 13: C03 Against the Second Version of UITCM

C03 Components	UITCM Components
-Automation.	AC04

-Trust Model.	HC02
-Standard Operating Procedure.	OC01
- Backup systems (Spatial /Temporal) Replication.	AC02
- Instrumental conditioning.	HC07
- Stimulation of risk perception.	HC06
- Collaborative Reinforcement Model.	HC03

Table 2. 14: C04 Against the Second Version of UITCM

C04 Components	UITCM Components
-Improve design of work environment	OC10
-Affordable access to mental health/drug treatment services .	OC07
-Appropriate time off for employees.	OC08
-Team-building activities to enhance mood.	OC9
-Incident-driven reviews (policies, practices, training materials).	OC14
-Improve design of user-system interfaces.	OC06
-Periodically, fully re-evaluate risk.	OC15
-Password protection.	AC05
-Wireless and Bluetooth safeguards.	AC06
-Email safeguards (anti-phishing, anti-malware), security information event management (SIEM).	AC07, AC08
-Anti-malware intrusion detection and prevention system (IDS/IPS) ,backup systems.	AC02,AC07, AC08,

In the above section, the focus has been on a critically comparing the proposed model against existing or source models. The comparison to the components of C01, C02, C03 and C04 proved that UITCM managed to support all components of the source models.

2.12 Small and Medium Enterprises

A worldwide definition of SMEs is lacking, and most academics have used their own definitions depending on their focus (Abdullah & Bakar, 2002). SMEs have been described by various academicians and researchers in Malaysia as the companies that have less than 200 associates and fixed assets worth approximately RM 2.5 million (Abdullah 2002; Salleh, 1991). The quantitative criteria formulated by Hashim and Abdullah (2000) defines SMEs in Malaysia using the following: (1) the companies are actively managed by the owners, i.e., "owner-managed or family business"; (2) it is mostly quite personalized, for instance an owner who has 77 management styles; (3) its operational area is typically quite narrow, and (4) it is mostly dependent on internal sources of capital for funding its growth.

To achieve the objectives of this study, small and medium enterprises (SMEs) were used because of their economic significance and because they are at higher risk of experiencing cyber security incidents.

A vital contribution is made by small and medium enterprises (SMEs) in economic development. SMEs all across the globe are considered as a major force that helps in bringing about innovation, economic growth, job opportunities, decreasing poverty and supporting large-scale organizations. It is reported that SMEs constitute over 50% of employment and 90% of the businesses worldwide. In addition, they constitute 45% of formal employment in developing nations (Kamal & Flanagan, 2014; Bauchet & Morduch, 2013). SMEs make a major contribution in the Malaysian economy and are recognized as the backbone of industrial development in the country (Saleh & Ndubisi, 2006). An average of 150 full-time workers are employed in small and medium enterprises and their yearly sales turnover is not more than RM25 million. They perform a vital role in the economic development of Malaysia,

particularly in the manufacturing sectors (Ramaya & Koay, 2002). It was found that by December 2005, a total of 600,000 SMEs were registered in Malaysia. They make a contribution of 27.3% to total manufacturing and 25.8% to value-added production. In addition, SMEs possess 27.6% of fixed assets and have employed 38.9% of the total workforce of the country (Alam & Noor, 2009).

Other distinct attributes of SMEs are that they typically give employment to generalists instead of specialists, depend to a greater extent on short-term planning, use dynamic and informal strategies and decision-making processes, and are hesitant in attaining rapid development and in using standard operating procedures. The key differentiator between SMEs and larger organizations is, however, the limited control of resources by SMEs, which is frequently known as "resource poverty". In addition, it is determined that in comparison to the larger organizations, SMEs are weaker at various levels, for example corporate, technological, individual managerial, environmental and individual. Therefore, the adoption and use of information technologies in SMEs is difficult (Ghobakhloo et al., 2012).

2.13 Model, Framework, Theoretical Framework and Conceptual Model

A conceptual framework (or simply framework) is a structure for the realization of a defined goal, and explaination relationships between variables of a study by arranged concepts that outline the input, process and output to change, develop or add the works (Méndez, 2012, p. 201). Framework explains the components, dimensions, limitations and directions of a study and presents the researcher's idea on how the research problem will have to be explored. A framework allows researcher to draw his own conclusions. It also supports logical, functional, computational, interaction, and application aspects.The conceptual framework is also called the research paradigm

(Andreson & Arsenault, 1998). A framework is "a set of ideas that researcher use when he is forming his decisions and judgements" (MacMillan English dictionary).

While theoretical framework describes the theoretical underpinnings of researcher work based on existing literatures. A framework is founded on the theoretical framework, which lies on a much broader scale of resolution. The theoretical framework dwells on time tested theories that embody the findings of numerous investigations on how phenomena occur. The theoretical framework provides a general representation of relationships between things in a given phenomenon (Creswell, 2012).

A model is a schematic form, often in a simplified way of an existing or future state or situation. A model is used to explain or represent a mechanism and operation of some process or a phenomenon. Model is representing a real-world object or phenomenon by a set of logical, mathematical and computational concepts and equations. It is a replacement of the original object. Model can be mathematical or computational model. Simulation of a system is the operation of a model (Lowyck,2014).

A Conceptual model is a diagram provides an easily understood representation of subject and describing the important information about an object, issue or system whether physical or social, in abstractical way; It is typically useful for communicating ideas to others. Conceptual models are used to help people know or understand a subject the model represents; it helps stakeholders better understand their situation. A conceptual model sets out the collective knowledge, experience and perspectives on the issue of interest. The model illustrates the assumptions about what are believed to be the important or dominant processes and their linkages. This includes the factors that are perceived to be driving the changes in the issue and the

consequences of changes in these factors. The conceptual model can be used as a keynote for solving a problem. The conceptual model allows us to look at a problem as if from the outside. Typically consists of named entities and their relationships to each other. A conceptual model should be accompanied by a textual description that verbally explains the conceptual model (Gustafson, 1996). A conceptual model is a logical structure of a theory or framework in a discipline (Jenny et al., 2015; Zamer&Scheiner, 2014). Conceptual models assist in developing and organizing sound explanations of core concepts (Anderson, 2008). It can be defined as a supporting structure around which something can be built or a system of rules, ideas or beliefs that is used to plan or decide something (Cambridge Advanced Learner's Dictionary).

Table 2. 15: Comparison of Model, Framework, Conceptual Model and Theoretical Framework

Model	Framework	Conceptual model	Theoretical Framework
Representing a real-world object or phenomenon. It is a graphical copy from an existed object, phenomenon or system.	Abstraction of things. It is does not exist in the real world. It is only exist in the mind of the researcher.	Abstraction of things. It is does not exist in the real world. It is only exist in the mind of the researcher.	Describes the theoretical underpinnings of researcher work based on existing literatures. A framework is founded on the theoretical framework.
Representing system or object behaviour to understand or to test the real object.	Framework explains the limitations of the work and how to be done to achieve a defined goal.	The conceptual model can be used as a keynote for solving a problem. The conceptual models help stakeholders better understand their situation.	Provides a general representation of relationships between things in a given phenomenon.

2.14 Appropriateness, Suitability and Usability

Model appropriateness depends on identifying the problem to be solved and the intended use of the model (usability), and requires evaluation of the model for goodness of fit (suitability) (Williams & Ette, 2002).

Suitability testing means testing whether a design has the right qualities for a particular purpose or situation and being appropriate according to the functional requirements without taking design principles into consideration. This entails a series of tests which perform a feature-by-feature validation of behaviour. Suitability testing can be conducted by involving users in a real experiment or by expert's evaluation. Suitability testing is more about 'product quality testing' than it is about 'usability' (Rouly et al., 2014). The objectives of suitability testing to a design are to: 1- Testing whether a design is logically consistent with the basic theories for which it was designed. 2- Testing if a design is theoretically valid. 3 -Testing if a design fulfils its purpose (Rouly et al., 2014).

Usability testing is the practice of testing how easy a design/product is to use with a group of representative users or area experts. Through usability testing, researcher can find design flaws and find solutions. By usability testing, researcher gets vital insights into how easy it is to use the product and not the product's quality. Then, researcher can leverage these insights to make improvements (Christoph et al., 2017). The objectives of usability testing to a design are to: 1- Is it able to be used? 2- How to use it? 3- Is it useful? 4- Is it understandable? Usability testing focuses on user acceptance and how well the user can use the product to complete the required task. Usability testing investigates all aspects of the usability of a product, including overall structure, navigational flow, layout of elements, and clarity of content and overall behaviour (Christoph et al., 2017).

2.15 Summary

The definitions of the terms and concepts pertinent to the issue of UITs have been presented in this chapter. This chapter discusses how these threats are linked to the information security system. The thesis topic and the three research questions presented served as a guide to make sure that there is a powerful relationship with the reviewed literature and the actual research study being carried out. The factors that are involved in UITs and their likelihood of occurring in organizations are discussed in this chapter. The UITs prevalent in Malaysian organizations were also discussed. The chapter provided a thorough review of the literature to understand the studies that have been carried out from various perspectives. Hence, the prevailing countermeasures of UITs and their limitations were elaborated so that the need for the proposed model could be comprehended. The research methodology and techniques used in the study will be discussed in the subsequent chapter.