CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter presents a summary of the research. It also provides a list of contributions that can be gained from the research, a discussion of some limitations of the study, and suggestions for future work to be done. The chapter ends with a brief summary of the study.

5.2. Research Recapitulation

Human errors are unavoidable and most problems related to computer security are happening due to people (Mazzarol et al., 2021; Whitman, 2004; Abu-Musa, 2006). In an organization, unintentional insider is the biggest insider threat of all, which means damage caused unintentionally by an employee. The review of existing countermeasure of Unintentional Insider Threats (UITs) showed that, they are insufficient; and the UITs cases in Malaysia still high. Defending UITs requires implementing multi layered defensive approaches including policies, procedures, technical controls, awareness, attention to sociology, psychology aspects and automated defence tools at all stages of the incident. Each one of the existing countermeasures addresses an aspect or some aspects of human errors. None of them have fully covered all countermeasures in all aspects, technological, organizational and human factors aspects. Thus the objective of this study is to propose a conceptual model as a countermeasure towards UITs by using Malaysian SMEs as a case study.

The initial version of the model was derived by combining the existing countermeasures that were identified from literatures. After development of the initial version of the model, a survey was conducted to check whether the model has covered all UIT issues especially in Malaysian organizations context. A total of 311 questionnaires were collected from IT Executives of the SMEs in Malaysia to determine the contributing factors and the likelihood of UITs. Quantitative data was analyzed using SPSS. The results of the analysis show that majority of the respondents from all the SME's alleged that their organizations were very likely to face threats with 634 (34.2%), which constituted approximately one-third of the respondents.

Also, 442 (23.9%) believed that their organizations were likely to confront this type of threats while 172 (9.3%) were most likely to face such threats. In addition based on the survey, ignorance and negligence (27%), situation awareness (26%) and human error (22%) were the most contributing factors of UIT in Malaysian organizations specifically in SMEs. Based on the contributing factors, the second version of UIT model was improved. All contributing factors have been mapped with the countermeasures so that the proposed model inclusively covered all contributing factors been identified. The updated version or known as a second version of the UITs model in the thesis is then further been evaluated. To evaluate the second version of the model, the Delphi method was used in order to reach acceptable level of agreement among experts and remove any uncertainty in the updated model. The experts were selected based on their experience in the study area that represent the theorists (academicians) and professionals (practitioners) from different international and local academic institutions, and industry with cybersecurity knowledge.

Based on the experts' review, in first round of the Delphi evaluation, several elements and components have been suggested to be improved or added. Then, the revised version of the UITs model has been presented to the experts in the second round of Delphi evaluation. According to the experts, the second version of the model was found to have relevant components; theoretically valid, usable, readable and understandable and they have collectively agreed with the final version of the UITs model.

Based on the feedback, the importance of this work lies on the use of the model as guidelines in organizations to assess the status of their UIT mitigation measures at every layer of the stack. It is hoped also that the model can be used to improve organization UIT countermeasures and indirectly strengthen their strategic, operational as well as financial of the organization.

5.3 Unintentional Insider Threats Countermeasure Model (UITCM) In Reducing Internal Threat Environment

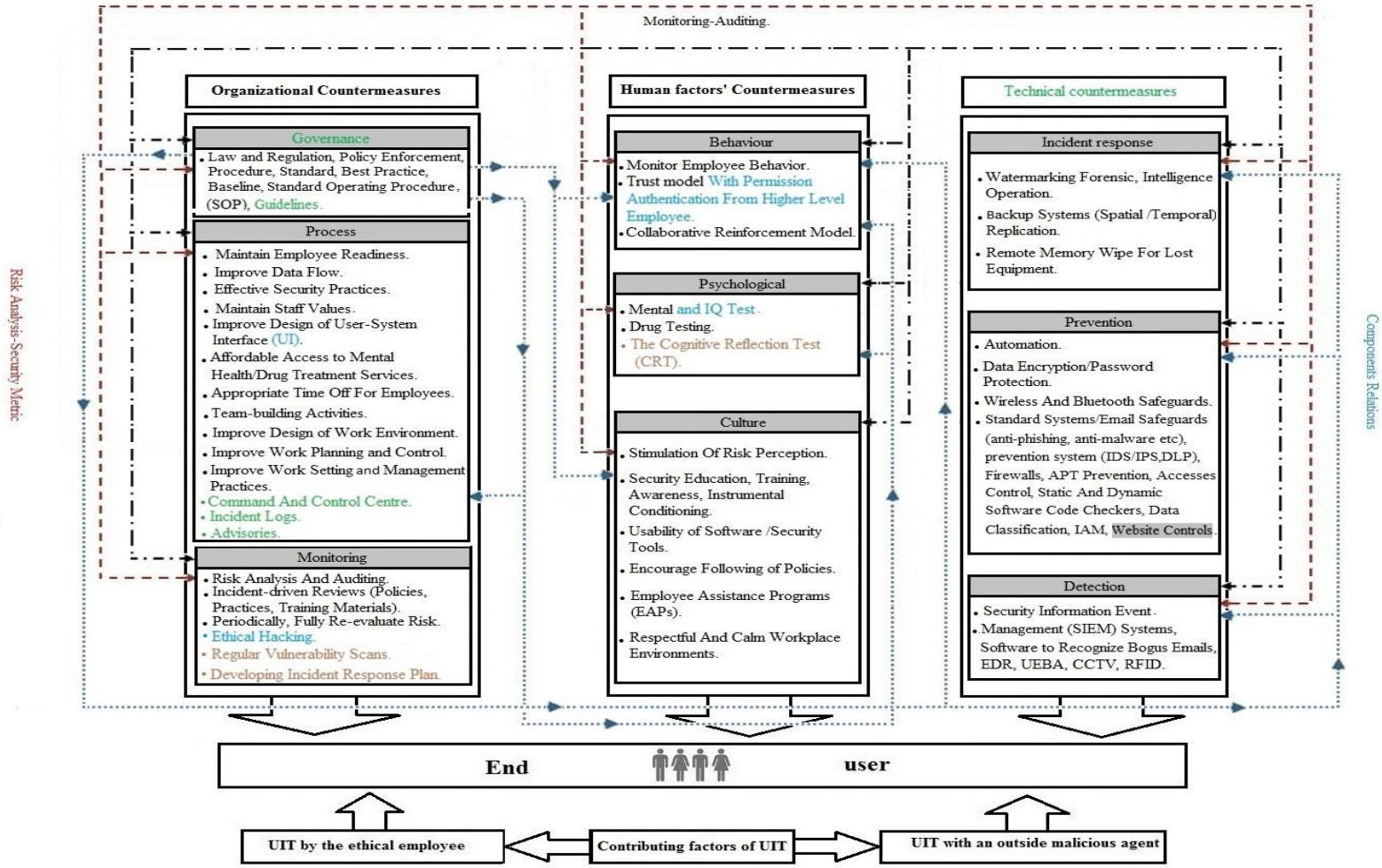

Figure 5. 1: Final version of UITCM

The initial version of the model was derived by combining the existing countermeasures that were identified from literatures. a survey was conducted toward IT Executives of the SMEs in Malaysia to determine the contributing factors of UITs in order to give them more focus and concern during the model development process and to ensure that they covered from all its aspects. UITCM includes nine groups of components which are; process, governance, monitoring, psychological, behaviour, culture, detection, prevention and incident response in three main domains; organizational countermeasures, human factor's countermeasures and technical countermeasures. Each group has its components such as governance group which includes eight components; Law and Regulation, Policy Enforcement, Procedure, Standard, Best Practice, Baseline, Standard Operating Procedure (SOP), Guidelines.

UITCM groups are connected with three types of relations; first relation between group and Monitoring and Auditing Processes, which represented by the dash-dotted line in black colour. Second relations between group and Risk Analysis and Security Metrics which represented by the dashed line in red colour. Third, relations among groups in UITCM which represented by the dotted line in blue colour. Each group is connected to other. For example psychological problems such as drug side effects and mental problems can negatively affect operator performance and can contribute to errors. Organization's laws and regulations should consider psychological problems of employees and thereby reducing the likelihood of the incidents related to working under the influence and encourages greater responsibility among employees who may cause harm to information system. Thus the UITCM proposed a relationship among psychological, behaviour, and managerial groups.

Where physiological state affects employee behaviour and managerial group is responsible for mitigating risks of physiological employee state, by some procedures

such as necessary tests and suitable work environments. For example if organization's laws and regulations impose mental abilities test and drug test as a condition of employment , potentially non-trustworthy candidates can be identified at the application stage and avoid those who may cause harm to information system. To see the details of UITCM components and its relations refer to Appendix I.

5.4 Research Contributions

Based on the finding of this study, theoretical contribution and practical implications are discussed in this section.

5.4.1 Theoretical Contributions

In the theoretical aspect this research contributes to the body of the knowledge.

A. Likelihood of UIT in Malaysian SMEs as a Case Study

The first contribution of the current research is the results from the survey that was conducted. The survey focuses on determining the likelihood level of UIT in Malaysian SMEs. The data were collected from 311 IT Executives of SMEs from technology MSC companies listed under InfoTech. The aim of this study tends to identify the likelihood level of unintentional insider threats in organizations especially in the perspective of IT Executives under InfoTech. The study showed the SME's executives' perception on the likelihood of UITs to occur in their organizations are very high. The results revealed that majority of the respondents from all the SME's alleged that their organizations were very likely to have faced threats with 634 (34.2%). Also, 442 (23.9%) believed that their organizations were likely to confront this type of threats while 172 (9.3%) were most likely to have faced such threats.

However, 332 (17.9%) and 272 (14.7%) responded that their organizations were not likely or least likely to face such threats respectively.

Therefore based on these data, it shows that the level of unintentional insider threats in Malaysian organizations required more attention and addition countermeasures of these threats are required.

B. Factors of UIT in Malaysian SMEs as Case Study

The second contribution of this research in theoretical aspect lies on the factors that lead to unintentional insider threats in Malaysian organizations. Based on the survey, the result shows that the majority of respondents (27%) characterized their incidents (UITs) arising from unintentional employee ignorance and negligence followed by situation awareness (26%) and human error (22%). The percentage of the others contributing factors were (mind wandering 2.2%, security policy enforcement 2.2%, mood 2.2%, culture 1.9%, budget of organization 1.6%, design of work environment 1.5%) respectively. The lowest percentage of UITs contributing factors were presented by management support 1.3%, gender 0.11%, motives and incentive and disincentive policy 0.90%, age effects 0.90%, stress and subjective mental workload 0.68%, risk possibility as personality feature 0.60%, fatigue and sleepiness 0.48%, influence of drugs and hormones 0.40% and apathy 0.30% respectively.

These identified factors can help the organizations to focus on doors of threats. The organizations can start strategizing their cybersecurity countermeasures so that it can match the most contributing factors of threats. For example, by creating awareness in the organizations on the direct and indirect causal factors of unintentional insider threats based on Malaysian SMEs case study, it can at least reduce number of cases to happen. Several preventing approaches can be determined

to help the organization especially when deals with threats that associated to human factors.

C. Contribution to Literature

This study serves as a reference for further research in the field of UIT countermeasures. This study identified the direct and indirect factors of UITs in Malaysian SMEs, such as; human error, fatigue and sleepiness, stress and subjective mental workload, situation awareness, skills and experience of employees, mind wandering, apathy, ignorance and negligence, motives and incentive and disincentive policy.. Etc. Then the study identified the existing countermeasures of these threats from the literature. The review of existing countermeasure showed that, they are insufficient; they did not fully cover all countermeasures in all aspects, technological, organizational and human factors aspects. This study created UITs multi layered defensive approaches including policies, procedures, technical controls, awareness, attention to sociology, psychology aspects and automated defence tools at all stages of the incident.

5.4.2 Practical Implications

In the practical aspect, this research helps organizations to implement the suitable UITs countermeasures and increase awareness on seriousness of UITs threats.

A. Unintentional Insider Threats Countermeasure Model (UITCM)

The main contribution of this research is the proposed Unintentional Insider Threats Countermeasures Model (UITCM). The research model is useful as a guideline and input to an organization to prevent from attacks and insider threats from further propagation. This work will assist IT Executives and organizations in

identifying the best countermeasure to combating cybercrime and securing their Information System. It is also beneficial related to awareness of human security threats countermeasures. The proposed model presented a wide group of countermeasures in three domains: technological, organizational and human factors aspects which were not addressed in the existing models and strategies. The model tried to cover the missing aspects in the existing models. The UITCM has addressed the gap of the literature. The model adopted multi layered defensive approaches by introducing policies, procedures , technical controls , awareness , attention to sociology , psychology aspects and automated defence tools at all stages of the incident which are prevent, detect and respond stage.

The model can be:

- Input to develop security framework, policy and guidelines to mitigate UITs and keep their information system safe.
- Use to identify awareness programs and improve security culture of organization as a medium to prevent and defend organization information security.
- Serve as guidance for creating a checklist to assess the status of their UIT mitigation measures and optimize their limited resources in ensuring security.

Due to the comprehensiveness of UITCM, it is hoped that it can be used by all organizations to help their employees in being safe online.

5.5 Limitation and Recommendation for Future Studies

This study has some limitations that will bring about the focus of subsequent research. First, the current research focuses only on using close-ended questions to

investigate the contributing factors of UITs in Malaysian SMEs. Therefore, subsequent studies can use open-ended questions to identify more contributing factors of UITs. Second, the current research focuses only on Executives of SMEs from technology MSC companies listed under InfoTech; hence, future studies may involve other Malaysian organizations. Third, the current study did not investigate the cultural differences, so subsequent studies may work on a comparison study with other countries. Fourth, this research focuses only on survey and literatures. Future studies can use an interview or observation, this may give more data and examples. Finally, the development of the model in this study was carried out using UITs countermeasures available until the time of achievement of this research, hence, subsequent studies can pay attention to the new UITs countermeasures in order to further refine and eliminate any weaknesses that the model might have.

A world with current new threats that keep complicating requires organizations and individuals to keep adapting to the new threats. Thus, researchers are required to always remain ahead of these challenges by investigating future threats. In this regard, researchers should keep update the likelihood level of UITs in Malaysian organizations with future studies and provide more data on Malaysian situation as the Malaysian documented references on UITs are scarcely found. Researchers should continue discovering more UITs countermeasures according to the new threats.

5.6 Summary

This research focuses on the development of UITCM in order to help the organizations to mitigate UITs. The countermeasures model has been developed based on the existing countermeasures in the literatures and the result of a survey that conducted to determine the likelihood level and contributing factors of UITs in

Malaysian SMEs. The result of the survey confirmed that the likelihood of UITs still high. According to the findings, the majority of the respondents from all the SME's acknowledge that their organizations were very likely to have faced threats. The result of this study shows that the majority of respondents (27%) characterized their incidents (UITs) arising from unintentional employee ignorance and negligence followed by situation awareness (26%) and human error (22%). The percentage of the others contributing factors were (mind wandering 2.2%, security policy enforcement 2.2%, mood 2.2%, culture 1.9%, budget of organization 1.6%, design of work environment 1.5%) respectively. The lowest percentage of UITs contributing factors were presented by management support 1.3%, gender 0.11%, motives and incentive and disincentive policy 0.90%, age effects 0.90%, stress and subjective mental workload 0.68%, risk possibility as personality feature 0.60%, fatigue and sleepiness 0.48%, influence of drugs and hormones 0.40% and apathy 0.30%. Furthermore, based on the results, the most contributing factors of UITs had be mapped as additional input to further develop the UITCM model. The model was developed in several stages. The initial version of the model was derived from literatures. Then the model was further improved as a second version based on the results of the survey conducted. The second version of the model was further been validated by experts' review and the Delphi method with addition inputs based on experts' suggestion during model evaluation to reach to the final version. The evaluation was done through the two rounds of Delphi to evaluate the theoretical validity, usability, readibilty and understandibility of the proposed UITCM. Delphi method is used to reach acceptable level of agreement among experts and remove any uncertainty in the model. According to the findings, the model was adequate and had relevant

components, the model includes logical connections, flows, and reasonable terms, and it is understandable.

These survey data also give an indication on doors of threats in most of Malaysian organizations. Determining the likelihood of UITs in Malaysian SMEs leads to more attention and taking threats seriously. The organizations must consider the contributing factors that may lead to UITs to can mitigate them early as possible. The organizations should create awareness on the direct and indirect causal factors of UITs and adopt modern technologies to mitigate UITs.

The results of this study have significant implications from the theoretical, practical and policy points of view. Therefore, the results of the study were able to bridge the existing gap in literature. Besides, the research model is useful for organizations to strategize their security defence and countermeasures, as the model adopted multi layered defensive approaches by introducing policies, procedures, technical controls, awareness, attention to sociology, psychology aspects and automated defence tools at all stages of the incident which are prevent, detect and respond stage. This in turn can strongly help organisations to employs awareness program to expand the security culture of organizations and as a guide to all the employees of the organization in being safe online.