UNINTENTIONAL INSIDER THREATS COUNTERMEASURE MODEL (UITCM) IN REDUCING INTERNAL THREAT ENVIRONMENT

ZAINAB. A. A. ABDELSADEQ

UNIVERSITI SAINS ISLAM MALAYSIA

UNINTENTIONAL INSIDER THREATS COUNTERMEASURE MODEL (UITCM) IN REDUCING INTERNAL THREAT ENVIRONMENT

Zainab. A. A.Abdelsadeq

Thesis submitted in partial fulfilment for the degree of
DOCTOR OF PHILOSOPHY IN
SCIENCE AND TECHNOLOGY

UNIVERSITI SAINS ISLAM MALAYSIA

March 2023

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 15 March, 2023

Signature :
Name : Zainab.A.A.Abdelsadeq
Matric No: 4140262
Address : Halaka alsharqiah. Box 9680, Sianah district, Taif 26551,3025,Saudi.A
Suleiman Al-Rajhi Street

ACKNOWLEDGEMENTS

All praises to Allah SWT for giving me the strength to complete this study.

A special gratitude and sincere appreciation goes to my supervisor and co-supervisors, Assoc. Prof. Dr. Nurlida Binti Basir, Dr.Syaril Nizam Omar and Dr.Nur Fatin Nabila Binti Mohd Rafei Heng for their guidance, generous advises, helpful comments, patience and great concern from the beginning till the end of study.

I wish to express my deepest appreciation to my dearest family members, especially to my parents, my husband, sister and brother, their support in this completed study. Also, I appreciate my friends who have given me support and encouragement during my Ph.D. research.

ABSTRAK

Ancaman orang dalam yang tidak disengajakan adalah salah satu isu terbesar yang boleh melemahkan pertahanan keselamatan organisasi.Kajian telah menunjukkan bahawa langkah balas keselamatan teknikal sedia ada sahaja tidak mencukupi terutamanya apabila ia berkaitan dengan kesilapan manusia. Oleh itu, dalam penyelidikan ini sebanyak 311 soal selidik telah dikumpul daripada Eksekutif Teknologi Maklumat Perusahaan Kecil Sederhana (PKS) di Malaysia untuk menentukan faktor penyumbang dan kemungkinan Ancaman Orang Dalam (UIT) yang tidak disengajakan.Data kuantitatif dianalisis menggunakan SPSS. Hasil analisis menunjukkan majoriti responden mendakwa organisasi mereka berkemungkinan besar menghadapi ancaman dengan 634 (34.2%), 442 (23.9%) percaya bahawa organisasi mereka berkemungkinan menghadapi ancaman jenis ini manakala 172 (9.3%) %) berkemungkinan besar telah menghadapi ancaman sedemikian.Di samping itu, kejahilan dan kecuaian (27%), kesedaran situasi (26%) dan kesilapan manusia (22%) merupakan faktor yang paling menyumbang kepada UIT dalam PKS Malaysia. Berdasarkan tinjauan, ia menunjukkan bahawa pendekatan defensif berbilang lapisan termasuk dasar, prosedur, kawalan teknikal, kesedaran, perhatian kepada sosiologi, aspek psikologi bersama dengan alat pertahanan automatik adalah penting bagi organisasi untuk melawan "isu rakyat". Pendekatan tunggal bagi tindakan balas hanya boleh menangani beberapa aspek kesilapan manusia tetapi bukan semua. Oleh itu, objektif kajian ini adalah untuk mencadangkan satu model yang terdiri daripada pendekatan campuran yang boleh digunakan sebagai langkah balas terhadap UIT terutamanya dalam PKS Malaysia. Model ini dibangunkan melalui beberapa peringkat. Versi pertama model yang dicadangkan telah dibangunkan dengan menggabungkan langkah balas sedia ada yang telah dicadangkan dalam literatur sedia ada. Pada peringkat kedua, model yang dicadangkan selanjutnya dinilai dengan menggunakan pertimbangan berasaskan pakar melalui kaedah Delphi dengan tujuan untuk mencapai tahap konsensus yang boleh diterima di kalangan pakar dan menghapuskan sebarang ketidakpastian dalam model. Lima (5) pakar dengan komposisi 3 pengamal dan 2 ahli akademik telah menilai model dengan soal selidik dua pusingan. Berdasarkan penilaian, keputusan menunjukkan bahawa pakar telah mencapai kata sepakat bersama dengan skor min melebihi 75% dari segi kesahan teori, kebolehgunaan dan kebolehbacaan dan kebolehfahaman model. Memandangkan tindakan balas ialah kawalan keselamatan yang digunakan untuk melindungi kerahsiaan, integriti, dan ketersediaan data dan sistem maklumat dan ia harus tersedia di setiap lapisan timbunan, diharapkan model itu boleh digunakan sebagai garis panduan oleh organisasi untuk menambah baik. langkah balas UIT sedia ada mereka dan secara tidak langsung mengukuhkan strategik, operasi serta kewangan organisasi mereka.

ABSTRACT

Unintentional insider threats (UITs) are one of the biggest issues that can weaken the security defence of the organization. Studies have shown existing technical security countermeasures alone are insufficient especially when it deals with human errors. A total of 311 questionnaires were collected from Information Technology Executives of the Small Medium Enterprises (SMEs) in Malaysia to determine the contributing factors and the likelihood of UITs. Quantitative data was analyzed using SPSS. The results showed majority of the respondents alleged that their organizations were very likely to have faced threats with 634 (34.2%), 442 (23.9%) believed that their organizations were likely to confront this threats. While 172 (9.3%) were most likely to have faced such threats. Ignorance and negligence (27%), situation awareness (26%) and human error (22%) were the most contributing factors of UIT in Malaysian SMEs. The survey showed that multi layered defensive approaches including policies, procedures, awareness, attention to sociology, psychology aspects together with automated defence tools are important to fight with the "people issue. Single approach of countermeasure can only addresses some aspects of human errors but not all. Thus the objective of this study is to propose a model that consists of mixed approaches that can be used as countermeasures to UITs in Malaysian's SMEs. The initial version of the proposed model was developed by combining the existing countermeasures that have been suggested in the literatures. In the second stage, the proposed model was evaluated by expert-based judgement through Delphi method to reach acceptable level of experts' consensus and remove any uncertainty in the model. Five (5) experts with the composition of 3 practitioners and 2 academicians have evaluated the model with two-round questionnaire. Based on the evaluation, the results indicated that the experts have reach mutual consensus with mean scores more than 75% in term of the theoretical validity, usability and readability and understandability of the model. Since countermeasure is a security control used to protect the confidentiality, integrity, and availability of data and information systems and it should be available at every layer of the stack, it is hoped that the model can be used as a guideline by the organizations to improve their existing UIT countermeasures and indirectly strengthen their strategic, operational as well as financial of the organization.

الملخص

تعتبر التهديدات الداخلية غير المقصودة من أكبر المشكلات التي يمكن أن تضعف الدفاع الأمني للمنظمة. أظهرت الدراسات أن التدابير الأمنية التقنية المضادة الحالية وحدها غير كافية خاصة عندما تتعامل مع الأخطاء البشرية. لذلك ، في هذا البحث ، تم جمع ما مجموعه 311 استبيانًا من مدراء تكنولوجيا المعلومات في الشركات الصغيرة والمتوسطة (SMEs) في ماليزيا لتحديد العوامل المساهمة واحتمالية التهديدات الداخلية غير المقصودة .(UITs) تم تحليل البيانات الكمية باستخدام برنامج SPSS.تظهر نتائج التحليل أن غالبية المستجيبين زعموا أن منظماتهم كانت على الأرجح قد واجهت تهديدات ، حيث اعتقد 634 (34.2٪) ، 442 (23.9٪) أن منظماتهم كانت عرضة لمواجهة هذا النوع من التهديدات بينما 172 (9.3٪) كانوا على الأرجح قد واجهوا مثل هذه التهديدات. بالإضافة إلى ذلك ، كان الجهل والإهمال (27٪) والوعي بالموقف (26٪) والخطأ البشري (22٪) من أكثر العوامل المساهمة في UIT في الشركات الماليزية الصغيرة والمتوسطة. بناءً على الاستطلاع ، يُظهر أن الأساليب الدفاعية متعددة الطبقات بما في ذلك السياسات والإجراءات والضوابط الفنية والوعي والاهتمام بعلم الاجتماع والجوانب النفسية جنبًا إلى جنب مع أدوات الدفاع الآلي مهمة للمؤسسة لمحاربة "قضية الأشخاص". يمكن للنهج الفردي للتدابير المضادة أن يعالج فقط بعض جوانب الأخطاء البشرية ولكن ليس كلها. وبالتالي ، فإن الهدف من هذه الدراسة هو اقتراح نموذج يتكون من مناهج مختلطة يمكن استخدامها كإجراءات مضادة تجاه الوحدات التي تعتمد على الروبوتات وخاصة في الشركات الصغيرة والمتوسطة في ماليزيا. تم تطوير النموذج عبر عدة مراحل. تم تطوير النسخة الأولى من النموذج المقترح من خلال الجمع بين التدابير المضادة الحالية التي تم اقتراحها في الأدبيات الحالية. في المرحلة الثانية ، يتم تقييم النموذج المقترح بشكل أكبر باستخدام الحكم القائم على الخبراء من خلال طريقة دلفي بهدف الوصول إلى مستوى مقبول من الإجماع بين الخبراء وإزالة أي عدم يقين في النموذج. قام خمسة (5) خبراء مع تكوين 3 ممارسين وأكاديميين بتقييم النموذج باستخدام استبيان من جولتين. بناءً على التقييم ، أشارت النتائج إلى أن الخبراء قد توصلوا إلى إجماع متبادل بمتوسط درجات أكثر من 75٪ من حيث الصلاحية النظرية وسهولة الاستخدام وقابلية القراءة والفهم للنموذج. نظرًا لأن الإجراء المضاد هو عنصر تحكم أمني يستخدم لحماية السرية والنزاهة وتوافر البيانات وأنظمة المعلومات ويجب أن يكون متاحًا في كل طبقة من المكدس ، فمن المأمول أن يتم استخدام النموذج كمبدأ توجيهي من قبل المنظمات لتحسين تدابيرها المضادة الحالية UIT وتعزز بشكل غير مباشر الاستراتيجية والتشغيلية وكذلك المالية للمنظمة.

TABLE OF CONTENTS

CHAPTER 5-CONCLUSION AND RECOMMENDATION

LIST OF TABLES

TABLES **PAGE**

LIST OF FIGURES

FIGURES **PAGE**

LIST OF APPENDICES

ABBREVIATIONS

IT	Information Technology
UIT	Unintentional Insider Threats
PDAs	Personal Digital Assistants
CERT	The Computer Emergency Response Team
CAS	Computerized Accounting Information Systems
GDP	Gross Domestic Product
I-O	Industrial-Organizational
SETA	Security Education Training Awareness
IS	Information System.
SME	Small and Medium Enterprise
ICT	Information and Communication Technology
ISM	Information Security Management.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DLP	Data Loss Prevention
APT	Advanced Persistent Threat
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
RF	Radio Frequency
P2P	Peer-to-Peer networks
WPAN	Wireless Personal area network
BYOD	Bring Your Own Device
EAPs	Employee Assistance Programs
CRT	The Cognitive Reflection Test
UI	User-System Interface
UITCM	Unintentional Insider Threats Countermeasure Model