UNIVERSITI TEKNOLOGI MARA

EVALUATING THE PERFORMANCE OF INVESTIGATION OFFICER IN SOLVING CYBERCRIME CASES

SYAMSYUL ANUAR BIN SAAD
TIMMY ANAK AHENG
NORHANA BINTI RAHMAN

Dissertation submitted in fulfilment
of the requirements for the degree of
Master in Business Administration

Arshad Ayub Graduate Business School

February 2024

ABSTRACT

Solving cybercrime cases within a stipulated time frame is a major Key Performance Indicator (KPI) among Investigation Officers (IO) and Assistant Investigation Officers (AIO) in the Royal Malaysia Police (RMP). This study seeks to understand the factors influencing IO and AIO in the State of Johor to solve cybercrime cases within the stipulated time frame. A cross-sectional study was undertaken to explore the potential relationship between motivation, attitude, workload and knowledge among IO and AIO in solving cybercrime cases. The primary data was collected through the distribution of a set of questionnaires to 72 officers in Johor. The responses from all respondents were analysed using Statistical Package for Social Sciences (SPSS). Descriptive and multivariate analysis were conducted. The majority of officers (88.0%) reported an average case-solving duration of 6 months, indicating that a significant portion encountered a 6-month timeframe in resolving cybercrime cases. The multivariate analysis revealed a positive correlation between attitude and knowledge, impacting the effectiveness of IO and AIO in handling cybercrime cases. However, motivation and workload were discovered to not influence the performance of IO and AIO. This suggests that while attitudes and knowledge are crucial factors in determining effectiveness and performance, motivation and workload might not be immediate influencers in this specific context of dealing with cybercrime cases. This study can assist RMP in refining their training programs to emphasise the development of attitudes and knowledge crucial for effectively managing cybercrime cases among IO and AIO. Additionally, it suggests that policies focusing solely on motivation and workload might not yield significant improvements in this specific context of cybercrime investigation.

ACKNOWLEDGEMENT

First and foremost, we express our thanks to the Almighty for giving us the opportunity to embark on our Master’s in Business Administration and for completing this long and challenging journey successfully.

Our deepest gratitude and thanks go to our supervisor, ***Associate Prof Dr Raja Adzrin Raja Ahmad,*** for her endless guidance, advice, knowledge sharing and expertise throughout our journey in completing this thesis.

We are grateful to the officers in the Commercial Crime Investigation Department, Johor, for spending their valuable time to participate in our study. Despite their commitment to daily jobs, they have given us cooperation, openness and professionalism throughout the way.

Finally, this thesis is dedicated to our loving family members and course mates who keep supporting us with positive vibes and encouraging us all the way.

Alhamdulillah.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 Chapter Overview

This chapter provides an overview of the study's dissertation. Section 1.2 begins with an introduction to the study, followed by Section 1.3, which elaborates on the background of the industry. Section 1.4 highlights the background of the organisation, and Section 1.5 elaborates on the problem statement. Section 1.6 discusses research questions, while the research objectives in Section 1.7. The scope and delimitation of the study are discussed in Section 1.8, while the significance of the study is discussed in Section 1.9. In Section 1.10, the limitation of the study is highlighted, followed by the definition of terms in Section 1.11. The chapter ends with Section 1.12, which discusses the definition of terms.

1.2 Background of the Study

In the new global economy, technology has evolved in every aspect of human life, regardless of the forms of the internet, computers, or cell phones. The advancement of technology has created an opportunity for scammers to commit various forms of cybercrime (Holt & Bossler, 2016). The term "cybercrime" is used to define various criminal activities in the virtual world, and its definition is influenced by cultural and legal factors (Verleysen, 2016). Another study by Kshetri (2013) identified that cybercrime is a form of criminal activity that exploits computers, computer networks, and the internet to commit offences or violate laws. This is supported by a study conducted by Furnell (2002) and McGuire and Dowling (2013) that interpret cybercrime as computer-focused crimes directly resulting from computer technology.

Meanwhile, Clifford (2001) and Wall (2002) defined cybercrime as high-tech crime or computer crime. Cybercrime is a complex and evolving issue encompassing a broad range of criminal activities facilitated by technology (Rush, 2009). It refers to criminal activities performed using computers, networks, and the internet, including a wide range of illegal and malicious activities. Moreover, it is conducted by individuals, groups, or even nations with a motive to cause harm, financial loss, or unauthorised