# Hasilian Research Snapshot

*by Ms. Noor Sabariah Salleh*

# BRING YOUR OWN DEVICE (BYOD) SECURITY COMPLIANCE MODEL VALIDATION USING HYBRID APPROACH

## Abstract

- This study aims to identify the risks of information security in Bring Your Own Device (BYOD) in the Malaysian public sector (MPS) due to non-compliance of security policies.
- It proposes countermeasure strategies and examines factors affecting employees' willingness to comply with BYOD security policies based on Protection Motivation Theory (PMT).
- The research uses a mixed-method approach, including interviews, document analysis, and surveys, with 21 respondents from the Malaysian public sector.
- The scope of this study is mainly focusing on BYOD implementation in Malaysian public sector (MPS) and the respondents are the employees who are working in government sectors including statutory bodies in Malaysia.
- The study aims to help organizations in MPS to be more prepared to establish BYOD security policies by studying employees' behaviour in complying with BYOD security policy requirements.

## Problem Statement

- Based on the Malaysian Administrative Modernization & Management Planning Unit (MAMPU) updated the new version of the Public Sector Information Security Policy in 2015, BYOD has been widely implemented by Malaysian government agencies to provide mobility, flexibility, increased productivity, and cost savings to the agencies.
- However, BYOD usage in the public sector has not been widely adopted because of a lack of understanding and acceptance of its advantages.
- It also poses security hazards to BYOD which include lack of security features on mobile devices, data leakage in shared media, data contamination due to mixed usage, and new types of malware targeting mobile devices.

## Research Questions

- What are the BYOD security risks raised by security policy non-compliance behaviour in the organization?
- What mitigation countermeasures can be considered in tackling the risks caused by security policy noncompliance behaviour?
- How do you identify the factors that influence an employee to comply with the BYOD security policy?

## Objectives

- To identify the BYOD information security risk faced in the MPS due to noncompliance behaviour of security policy.
- To analyse the countermeasure strategies for handling the BYOD risks in technical and non-technical security measures.
- To evaluate the validity of the PMT research model in identifying the factors that influence an employee in complying with BYOD security policy.

## Framework

### Based on The Protection Motivational Theory (PMT) – Rogers, 1975

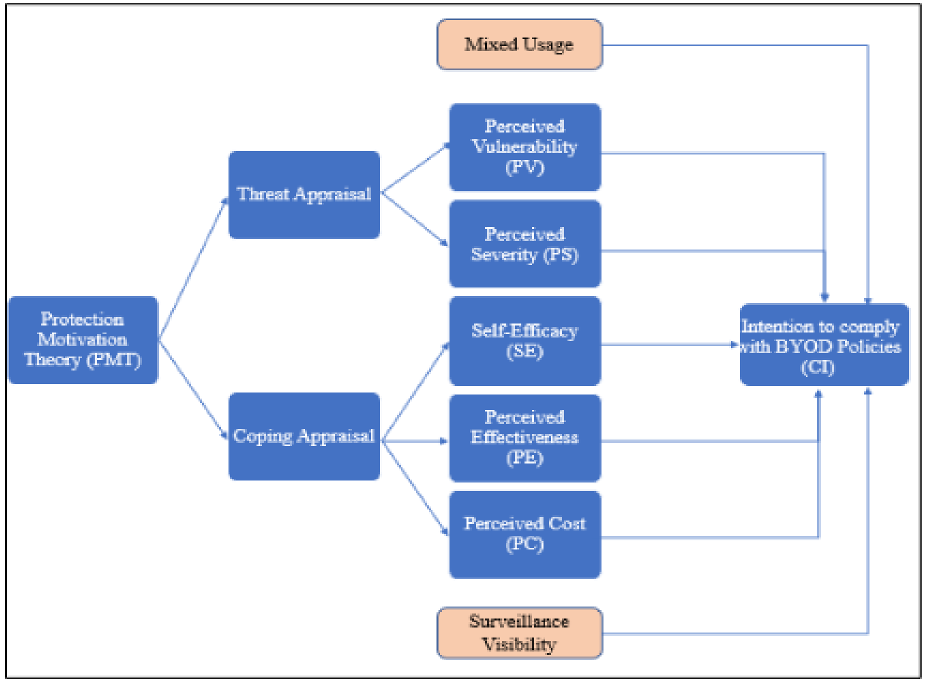
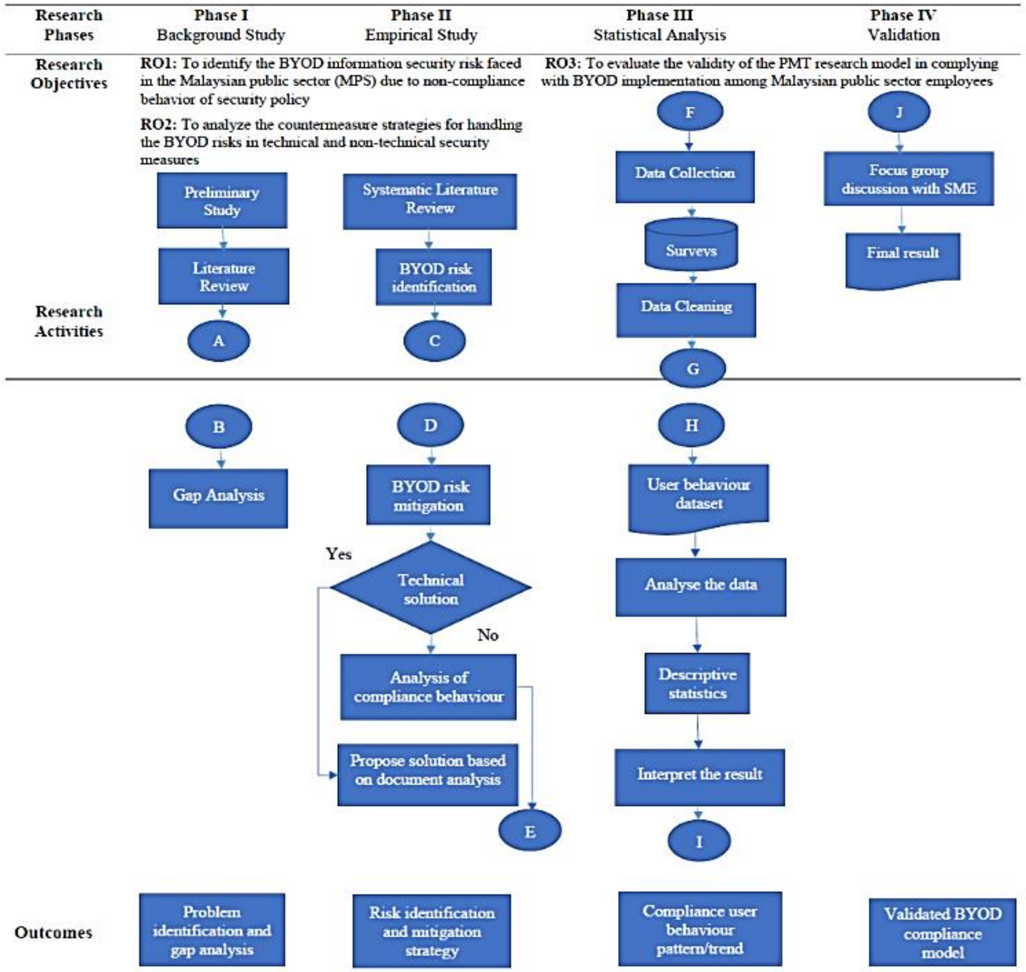

Mixed Usage
Threat Appraisal
Perceived Vulnerability (PV)
Perceived Severity (PS)
Protection Motivation Theory (PMT)
Self-Efficacy (SE)
Intention to comply with BYOD Policies (CI)
Coping Appraisal
Perceived Effectiveness (PE)
Perceived Cost (PC)
Surveillance Visibility

**Diagram 1: PMT Research Model**

- According to PMT, an individual's reaction to a threat is the result of two appraisal processes: **threat appraisal** and process of **coping appraisal.**
- Based on PMT, a study model was built in proposing that both threat and coping assessments influence an employee's intention to follow the organization's BYOD security policy together with BYOD unique features such as surveillance visibility and mixed usage.



**RO1:** To identify the BYOD information security risk faced in the Malaysian public sector (MPS) due to non-compliance behavior of security policy

**RO2:** To analyze the countermeasure strategies for handling the BYOD risks in technical and non-technical security measures

**RO3:** To evaluate the validity of the PMT research model in complying with BYOD implementation among Malaysian public sector employees

Research Activities
Preliminary Study
Literature Review
A
Systematic Literature Review
BYOD risk identification
C
F
Data Collection
Surveys
Data Cleaning
G
J
Focus group discussion with SME
Final result
B
Gap Analysis
D
BYOD risk mitigation
Yes
Technical solution
No
Analysis of compliance behaviour
Propose solution based on document analysis
E
H
User behaviour dataset
Analyse the data
Descriptive statistics
Interpret the result
I
Outcomes
Problem identification and gap analysis
Risk identification and mitigation strategy
Compliance user behaviour pattern/trend
Validated BYOD compliance model

**Diagram 2: Research Framework**

## Methodology

- This study is based on a mixed-method research approach whereby both qualitative and quantitative data collection techniques are used. Data collection method used includes interviews, document analysis and surveys with 21 valid respondents.

## Findings

1. BYOD security risks:

- The risk identified from the review is mapped according to the **People, Process and Technology (PPT)**.
- **People**: Discontented employee could become internal threat to an organization (victims of phishing and sharing data using insecure public networks).
- **Process**: Policy and education.
- **Technology**: Device management, application and data security as well as technical issues.

2. Mitigation countermeasures in tackling the risks:

- Awareness and training for employees to understand and manage personal devices.
- Create a healthy work environment and a good security policy for establishing and maintaining a secure IT environment.
- Technical countermeasures include deploying Mobile Device Management, asset management, network platform controls, strong passwords, encryption, surveillance and monitoring.

3. To identify the factors that influence an employee to comply with the BYOD security policy:

- 73.8% of the variance in an employee’s intention to comply with BYOD security policies was explained by the PMT model.
- Coping action self-efficacy and surveillance visibility were found to have a significantly positive relationship with intentions to comply with BYOD security policies. The strength of the linear link between two variables is indicated by the correlation coefficient.

## Conclusion

- The threat appraisal of the employee, which includes perceived vulnerability and perceived severity, and the coping appraisal of the employee, which includes self-efficacy, perceived effectiveness, and perceived cost, have a major impact on the employee's desire to comply.
- The PMT has proved that 73.8% of the intention to comply with BYOD security policies is mainly due to the perceived vulnerability, perceived severity, coping action self-efficacy, perceived effectiveness, perceived cost, mixed usage, and surveillance visibility .
- The findings can help organizations implement effective BYOD security policies, enhancing protection of organizational information assets and strengthening the "People" pillar.
- The research is crucial for understanding BYOD behaviour and policy implementation.

## Research Gap

- This study has limitations due to its survey respondents being from federal government and statutory bodies, excluding state governments in Malaysia's public sector.
- The findings may not be widely applicable due to different work cultures and environments.
- Additionally, the study only focuses on two unique BYOD features, which may be influenced by other factors due to rapid mobile technology development.