HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Vol. 9, No. 1, (2025)

A Conceptual Framework: Employee Behavior and Risk Mitigation in Cybersecurity for Omani SMEs

Fahad Abdullah Saif Al Abri, a) and Setyawan Widyarto*, b)
*Corresponding author

(a) 1,2Department of Computing
Faculty of Communication, Visual Art and Computing,
Universiti Selangor, Selangor, Malaysiae.

Author Emails
a) alscoon2@gmail.com
b)swidyarto@unisel.edu.my, ORCID iD: 0000-0002-6317-9875

Abstract: The rise in cyber threats faced by Small and Medium Enterprises (SMEs) due to inadequate cybersecurity measures, particularly from insufficient employee awareness, limited resources, and outdated security infrastructures, has led to financial and reputational risks. This research addresses the problem of SMEs lacking robust cybersecurity frameworks, making them vulnerable to cyberattacks. The study aims to empirically evaluate the mediating role of information security behaviour types between risk factors, threat factors, and cybersecurity effectiveness in Omani SMEs. A quantitative research approach will be employed, involving surveys to collect data on key cybersecurity variables from a sample of 372 non-managerial employees, determined using the Raosoft sample size calculation model. Data analysis will involve statistical techniques such as Structural Equation Modelling (SEM) and mediation analysis. The findings of this research are expected to provide valuable insights into how SMEs in Oman can enhance cybersecurity strategies, mitigate risks, and foster a more cyber-secure organisational culture. The study will also contribute to developing practical guidelines for SMEs to strengthen cybersecurity awareness, improve risk management strategies, and ensure long-term digital resilience. Ultimately, this research offers actionable recommendations for SMEs, policymakers, and cybersecurity practitioners to enhance cybersecurity awareness and improve risk mitigation strategies.

Keywords: Cybersecurity, SMEs (Small and Medium Enterprises), Information Security Behaviour, Risk and Threat Factors

1. Introduction

In an era of escalating cyber threats, organizations of all sizes face significant security challenges. Small and Medium Enterprises (SMEs) are particularly vulnerable due to inadequate cybersecurity measures, limited resources, insufficient employee awareness, and outdated infrastructure—factors that expose them to financial and reputational risks. This study addresses a critical issue in Oman: the lack of robust cybersecurity frameworks in SMEs, which increases their susceptibility to cyberattacks.

While modern technology enables flexible work arrangements through cloud computing, mobile devices, and remote access, it also introduces new security risks. Human factors—such as indifference to security guidelines, perceived effort in compliance, and unintentional errors—often create vulnerabilities, making employees the weakest link in data protection. Recognizing this, our research empirically examines the mediating

role of information security behavior types in the relationship between risk factors, threat factors, and cybersecurity effectiveness in Omani SMEs. By doing so, we aim to provide actionable insights to strengthen cybersecurity strategies, mitigate risks, and foster a more secure organizational culture.

1.1. Background and Problem Statement

The increasing reliance on digital solutions has made businesses, including Omani SMEs, more exposed to cyber threats. Cybercriminals frequently target SMEs due to their weaker defenses, leading to severe consequences such as financial losses, reputational harm, and even business closures. A key challenge lies in employee behavior—many security breaches stem from a lack of awareness about the risks associated with careless actions. This study seeks to investigate how risk and threat factors influence cybersecurity in Omani SMEs and how information security behaviors mediate this relationship.

1.2. Research Questions and Objectives

To guide this investigation, we address the following research questions:

- How do risk and threat factors affect cybersecurity in Omani SMEs?
- How do risk and threat factors influence information security behavior types in Omani SMEs?
- What is the relationship between information security behavior types and cybersecurity in Omani SMEs?
- To what extent do information security behavior types mediate the impact of risk and threat factors on cybersecurity in Omani SMEs?

The corresponding research objectives are:

- To assess the impact of risk and threat factors on cybersecurity.
- To evaluate the effect of risk and threat factors on information security behavior types.
- To analyze the relationship between information security behavior types and cybersecurity.
- To determine the mediating role of information security behavior types in the link between risk/threat factors and cybersecurity.

1.3. Scope and Methodology

This study focuses on non-managerial employees in Omani SMEs. Data will be collected from 372 respondents via a structured survey measuring risk factors, threat factors, information security behaviors, and cybersecurity effectiveness. Statistical analyses—including regression and mediation analysis—will be employed to test the hypothesized relationships.

1.4. Significance of the Study

This research contributes to the understanding of employee-driven cybersecurity risks in SMEs. The findings will help managers and policymakers enhance security measures by identifying key behavioral influences, improving training programs, and developing targeted cybersecurity strategies. Ultimately, this study aims to strengthen the resilience of Omani SMEs against evolving cyber threats.

2. Literature Review

While technological advancements play a crucial role in defending Small and Medium Enterprises (SMEs) against data breaches and cyber threats, over-reliance on technical solutions overlooks a critical vulnerability: human behavior. Research increasingly recognizes that employees—through both intentional and unintentional actions—significantly influence cybersecurity outcomes. Studies emphasize the importance of non-technical measures, integrating behavioral insights into information security frameworks to better understand how human factors contribute to organizational vulnerabilities.

Several theories have been proposed to explain employee behavior in cybersecurity contexts. Among these, the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) provide robust frameworks for analyzing how individuals' attitudes, perceived norms, behavioral control, and threat assessments shape their security-related actions. While prior research often uses behavioral intention as a proxy for actual behavior, a persistent gap remains between intention and real-world actions. This discrepancy highlights the need for direct examination of cybersecurity behaviors rather than relying solely on predictive models.

Understanding human behavior in cybersecurity is complex, with existing models often limited by industry-specific or theory-bound constraints. To address this, recent studies categorize information security behaviors into distinct types:

- Deliberate naïve/accidental behaviors (unintentional security lapses due to lack of awareness)
- Risk-averse behaviors (cautious actions driven by threat perception)
- Deliberate risk-inclined behaviors (intentional disregard for security protocols)

These behavioral distinctions help explain why some employees adhere to cybersecurity measures while others—whether through negligence or deliberate actions—undermine them.

Employees' perceptions of risk significantly influence their cybersecurity behaviors. Key factors identified in prior research include:

- Perceived susceptibility (likelihood of a threat affecting them)
- Perceived severity (potential impact of a security breach)
- Certainty of detection (belief that violations will be noticed)
- Severity of punishment (expected consequences of non-compliance)
- Effort required for compliance (perceived difficulty in following security protocols)

Understanding these factors is essential for developing effective cybersecurity strategies, as they shape how employees engage with security measures.

This section details the study's positivist, quantitative approach, cross-sectional design, sampling strategy, and analytical techniques. By employing rigorous statistical methods, the research aims to validate its conceptual framework and provide actionable insights into cybersecurity behaviors in Omani SMEs.

2.1. Research Gap and Contribution

While existing studies explore risk perceptions and security behaviors independently, few examine how information security behavior types mediate the relationship between risk/threat factors and overall cybersecurity effectiveness—particularly in Omani SMEs. This study bridges that gap by integrating TPB and PMT into a unified framework, empirically testing how employee behaviors influence cybersecurity outcomes.

2.2. Small and Medium Enterprises (SMEs) in Oman

SMEs are crucial for a nation's economic prosperity, driving industrial growth and technical innovation. While the definition of SMEs varies across countries, in Oman, an SME is typically classified as an institution with less than 100 employees and a revenue below RO 3 million (SMEF, 2017). As of January 2016, further classification in Oman includes Micro (1-5 employees, < RO 100,000 annual sales), Small (6-25 employees, RO 100,000 - 500,000 annual sales), and Medium (26-99 employees, RO 500,000 - < RO 3,000,000 annual sales). A significant number of SMEs are registered in Oman, with a notable concentration in Muscat. SMEs often face unique challenges, particularly limited resources during their development, which can hinder their ability to implement robust information technology (IT) and cybersecurity systems.

2.3. Cybersecurity in the Context of SMEs

Cybersecurity is defined as a method to ensure an artefact's safety from physical damage, unauthorized access, theft, or loss by maintaining high anonymity and integrity, and ensuring information availability when needed (Khan, Khan, & Pandey, 2020). It involves recognizing cyber risks and implementing defensive measures. SMEs are increasingly becoming targets for cybercriminals who exploit their often weaker security systems. This is a shift from the past when many SMEs believed they were too small to be targeted (Caldwell, 2016). However, the evolving sophistication of cyber threats necessitates that SMEs become more aware of the potential financial and reputational damage resulting from cyberattacks (Jayakumar, 2020). Data breaches can lead to substantial financial losses and erode customer trust. Therefore, it is crucial for SMEs to protect themselves, identify security threats, and develop effective response strategies (Dellmuth et al., 2018). Research indicates various themes related to cybersecurity in SMEs, including their awareness of cyber threats, mitigation strategies, readiness, supply chain security, regional studies on cyber risks, social engineering threats, and information security practices. Despite the growing importance, cybersecurity in SMEs, particularly concerning employees' behaviour, has received limited research attention (Donalds & Osei-Bryson, 2020; Khan et al., 2022). This highlights the need to understand risk and threat factors and employee information security behaviour affecting cybersecurity in this context.

2.4. Employee Perceived Risk and Threat Factors Towards Cybersecurity

The internet's significant societal impact has transformed modern life, but security measures have often lagged behind technological advancements (Castells, 2008; Donsbach & Traugott, 2007; Gupta & Shakya, 2015). A lack of research in information security emphasizes the need for further studies on risks and threats in the technology environment, encompassing both technical and non-technical measures like user training and behaviour understanding (Chen, Ramamurthy, & Wen, 2015; Ernest Chang & Lin, 2007). Consequently, disciplines like organizational behaviour, psychology, and sociology are increasingly integrated into information security studies to address non-technical aspects (Chu & Chau, 2014). The perception of imminent threats varies among individuals, and individual expectations, along with preventive factors, significantly influence responsible behaviour. This study focuses on the link between perceived risk and threat factors and cybersecurity, recognizing that despite technological advancements, vulnerabilities persist due to the human factor (Anwar et al., 2017; Herath & Rao, 2009). The Protection Motivation Theory (PMT) is highlighted as offering new insights into employees' perceived risk and threat factors in the workplace. Previous research has identified several factors in this domain, such as perceived severity, perceived vulnerability, perceived barriers, response efficacy, self-

efficacy, peer behaviour, and cues to action (Li et al., 2019; Anwar, He, Ash, et al., 2017). This study specifically aims to apply five employee-perceived risk and threat factors: perceived susceptibility, perceived severity, perception of the certainty of detection, perception of the severity of punishment, and perception of effort to safeguard.

2.5. Information Security Behaviours Towards Cybersecurity

Information security behaviour refers to the range of actions individuals demonstrate when using computers for work (Pattinson et al., 2016). These behaviours can be categorized into deliberate naive and accidental behaviours, risk-averse behaviours, and deliberate risk-inclined behaviours. Snyman and Kruger (2019) developed a taxonomy with six elements, categorizing behaviours based on intent and skill, noting that higher intent often requires higher skill levels. Stanton et al.'s (2005) taxonomy also provides a basis for understanding different categories of information security behaviours. This study focuses on:

- Naive and Accidental Behaviours: Employees with limited cybersecurity knowledge who may unintentionally compromise security through actions like clicking suspicious links.
- Deliberate Risk Averse Behaviours: Intentional actions to protect information systems, often influenced by group norms and openly practiced (Snyman & Kruger, 2019).
- Deliberate Risk Inclined Behaviours: Intentional actions that disregard security protocols, potentially due to various motivations. Understanding these behaviour types is crucial for developing effective strategies to influence actions and build a robust cybersecurity framework (Hutchison, 2018).

2.6. Theoretical Perspective

This research draws upon two dominant theories in cybersecurity studies: Protection Motivation Theory (PMT) and Theory of Planned Behaviour (TPB) . PMT suggests that individuals' protective behaviours are driven by threat appraisal (perceived susceptibility and severity) and coping appraisal (response efficacy and self-efficacy) (Rogers, 1975; Norman et al., 2015). In the context of Omani SMEs, perceived susceptibility and severity of cyber threats can motivate employees to adopt information security behaviours. PMT provides a framework to understand how risk and threat factors influence information security behaviour types and, consequently, cybersecurity in Omani SMEs. Individuals perceiving higher susceptibility and severity are more likely to adopt risk-averse behaviours. TPB posits that behaviour is determined by attitudes towards the behaviour, subjective norms, and perceived behavioural control (Ajzen, 1985; Kashif, Zarkada, & Ramayah, 2018). In cybersecurity, TPB can explain how the perception of detection certainty, punishment severity, and effort to safeguard influences employees' intentions and behaviours. Combining these theories offers a more comprehensive understanding of the motivations and factors influencing cybersecurity behaviours.

2.7. Past Studies

Past empirical studies in information and cybersecurity fields inform the current research (Anwar, He, Ash, et al., 2017; Donalds & Osei-Bryson, 2020; Chatterjee, Kar, & Gupta, 2017). Research has highlighted the importance of understanding risks associated with weak online security behaviours (Li et al., 2019). Studies have also examined the human factor as a significant vulnerability in information security (Anwar et al., 2017; Herath

& Rao, 2009). Research in Oman has explored factors influencing protection intentions in BYOD environments, finding attitude and perceived vulnerability as strong determinants (Al-Harthy & Ali, 2022; Al-Harthy et al., 2019). Furthermore, studies have reviewed global challenges faced by SMEs and survival strategies, emphasizing the vital role of SMEs in the global economy (Naradda Gamage et al., 2020). Research in Kenya has shown a connection between evaluating information security risks and company performance (Ndungu et al., 2018). Studies in the Dhofar region of Oman have examined ICT adoption by SMEs, identifying barriers such as lack of financial resources and technical expertise (Hussein, Ahmed, & Alraja, 2017). Research in Bahrain has identified critical cybersecurity threats faced by organizations (Al-Alawi, Al-Bassam, & Mehrotra, 2020). These diverse studies underscore the complexity of cybersecurity in SMEs and the importance of considering human factors and contextual elements.

2.8. Conceptual Framework and Hypotheses

This research proposes a conceptual framework (Figure 2.1) that examines the mediating effect of information security behaviour types on the relationship between risk and threat factors and cybersecurity in Omani SMEs. Based on this framework, the following hypotheses are proposed:

- Hypothesis 1: Risk and threat factors (perceived susceptibility, perceived severity, perception of the certainty of detection, perception of the punishment severity, perception of effort to safeguard) have a significant effect on cybersecurity in Omani SMEs.
- Hypothesis 2: Risk and threat factors (perceived susceptibility, perceived severity, perception of the certainty of detection, perception of the punishment severity, perception of effort to safeguard) have a significant effect on information security behaviour types (naive and accidental behaviour, deliberate risk averse behaviour, deliberate risk inclined behaviour) in Omani SMEs.
- Hypothesis 3: Information security behaviour types (naive and accidental behaviour, deliberate risk averse behaviour, deliberate risk inclined behaviour) have a significant effect on cybersecurity in Omani SMEs.
- Hypothesis 4: Information security behaviour types (naive and accidental behaviour, deliberate risk averse behaviour, deliberate risk inclined behaviour) mediates the relationship between risk and threat factors (perceived susceptibility, perceived severity, perception of the certainty of detection, perception of the punishment severity, perception of effort to safeguard) and cybersecurity in Omani SMEs.

This section reviewed the relevant literature on cybersecurity in SMEs, focusing on the interplay between risk and threat factors, employee information security behaviours, and overall cybersecurity posture, particularly within the Omani context. The review highlighted the increasing vulnerability of SMEs, the critical role of human behaviour in cybersecurity, and the applicability of Protection Motivation Theory and Theory of Planned Behaviour in understanding these dynamics. The proposed conceptual framework and hypotheses lay the groundwork for the empirical investigation detailed in the subsequent sections.

3. Methodology

This section outlines the methodological framework guiding the study, detailing the research paradigm, approach, design, data collection, and analysis procedures. A robust methodology is essential to ensure the study effectively addresses its research questions and objectives.

3.1. Research Paradigm and Approach

The study adopts a positivist paradigm, emphasizing objective reality, measurable variables, and quantitative analysis. This aligns with the study's goal of empirically testing relationships between risk/threat factors, information security behaviors, and cybersecurity effectiveness. A deductive approach is employed, where hypotheses derived from existing theories (e.g., Protection Motivation Theory, Theory of Planned Behavior) are tested through structured data collection and statistical analysis.

3.2. Research Design and Time Horizon

The study follows a cross-sectional, explanatory design, capturing data at a single point in time to examine the relationships between variables. While longitudinal studies track changes over time, this approach balances efficiency with rigor, providing timely insights into cybersecurity behaviors in Omani SMEs. The design is quantitative, using survey-based methods to collect numerical data for statistical testing.

3.3. Population and Sampling

The target population consists of non-managerial employees in Omani SMEs, estimated at 11,000 individuals (Global Entrepreneurship Monitor, Oman). A sample size of 372 was determined using Raosoft's sample size calculator, ensuring a 95% confidence level and 5% margin of error. Probability sampling will be applied to give each population member an equal chance of selection, enhancing representativeness.

3.4. Data Collection Instrument

Data will be collected via an online questionnaire divided into two sections:
Section A: Demographic information (nominal/ordinal scales).
Section B: Variables measured on a 5-point Likert scale ("strongly disagree" to "strongly agree"), including:

- Risk/threat factors: Perceived susceptibility, severity, certainty of detection, punishment severity, and effort to comply.
- Information security behaviors: Naive/accidental, deliberate risk-averse, and deliberate risk-inclined behaviors.
- Cybersecurity effectiveness: Implementation of security controls and incident frequency.

3.5. Pilot Study and Reliability

A pilot test (n=30) confirmed the questionnaire's clarity and reliability. Cronbach's alpha coefficients (>0.7 for all variables) demonstrated strong internal consistency, leading to final refinements.

3.6. Data Analysis

Data will be analyzed using SPSS and Smart-PLS:

- SPSS: Descriptive statistics, normality tests, outlier detection, and demographic analysis.
- Smart-PLS: Structural Equation Modeling (SEM) to assess:
- Path coefficients (β) and significance (p-values) for hypothesized relationships.
- Mediation effects of information security behaviors.
- Explanatory power (R^2) of the model.

3.7. Ethical Considerations

Participation will be voluntary, with informed consent.

Anonymity and confidentiality of responses will be maintained.

4. Expected Findings

This research expects to find a significant positive relationship between risk and threat factors and cybersecurity in Omani SMEs, suggesting that a higher perception of risk and threats leads to better cybersecurity practices. Furthermore, a significant relationship is anticipated between risk and threat factors and information security behavior types, indicating that perceived risks and threats influence how employees behave in relation to information security. It is also expected that information security behavior types will significantly impact cybersecurity, with risk-averse behaviors leading to improved cybersecurity outcomes. Crucially, this study anticipates finding that information security behavior types mediate the relationship between risk and threat factors and cybersecurity in Omani SMEs, suggesting that employees' behaviors act as a crucial link in translating risk awareness into effective cybersecurity.

4.1. Potential Contribution

This research has the potential to contribute to both theory and practice:

• **Theoretical Contributions:** This study aims to validate the hypotheses of the cybersecurity framework in Omani SMEs by examining employee behavior. It contributes to the field of information systems by addressing the research gap in cybersecurity and proposing and testing an enhanced model incorporating the mediating effect of information security behavior types. By drawing upon the Protection Motivation Theory and the Theory of Planned Behavior, this research can assess the validity and reliability of the cybersecurity framework in this specific context.

•**Practical Contributions:** The findings of this research can provide practical guidelines for SMEs in Oman to strengthen their cybersecurity strategies. By understanding the influence of risk and threat perceptions on employee behavior and subsequently on cybersecurity, SMEs can develop targeted interventions to enhance cybersecurity awareness and promote risk-averse behaviors. The study can also inform policymakers about the key factors influencing cybersecurity in the SME sector, enabling the development of more effective support and regulatory frameworks. Ultimately, this research offers actionable recommendations for SMEs, policymakers, and cybersecurity practitioners to enhance cybersecurity awareness and improve risk mitigation strategies.

5. Conclusion

This proposed research seeks to provide a comprehensive understanding of the intricate relationship between risk and threat factors, employee information security behavior types, and cybersecurity effectiveness within the context of Omani SMEs. By employing a quantitative methodology and drawing upon established behavioral theories, this study aims to empirically validate the mediating role of employee behavior in translating risk awareness into tangible cybersecurity improvements. The expected findings hold significant theoretical and practical implications, offering valuable insights for SMEs, policymakers, and cybersecurity professionals in enhancing cybersecurity posture and fostering a more resilient digital environment in Oman.

Acknowledgments

The authors would like to express their sincere gratitude to Universiti Selangor for the academic support and guidance provided throughout the development of this proposal. Special thanks are extended to the faculty members of the Department of Computing, Faculty of Communication and Computing, for their valuable insights and encouragement. We also wish to acknowledge the assistance and cooperation received from various Small and Medium Enterprises (SMEs) in Oman, whose participation and feedback have been instrumental in shaping the direction of this study on employee behavior and cybersecurity risk mitigation.

References

Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020). Critical cybersecurity threats: Frontline issues faced by Bahraini organizations. In Implementing computational intelligence techniques for security systems design (pp. 210–229). IGI Global. https://doi.org/10.4018/978-1-5225-9746-9.ch010

Al-Harthy, I. M., & Ali, N. A. (2022). Determinants of BYOD protection behavior: An employee's perspective. Journal of Theoretical and Applied Information Technology, 100(13), 1–12. http://www.jatit.org/volumes/Vol100No13/1Vol100No13.pdf

Al-Harthy, I. M., Rahim, F. A., Ali, N. A., & Singun, A. P. (2019, December). Theoretical bases of identifying determinants of protection intentions towards bring-your-own-device (BYOD) protection behaviors. In 2019 First International Conference of Intelligent Computing and Engineering (ICOICE) (pp. 1–9). IEEE. https://doi.org/10.1109/ICOICE48418.2019.9035132

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Chu, A. M., & Chau, P. Y. (2014). Development and validation of instruments of information security deviant behavior. Decision Support Systems, 66, 93–101. https://doi.org/10.1016/j.dss.2014.06.007

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management, 51, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hussein, M. A., Ahmed, H. M. S., & Alraja, M. N. (2017). The adoption of information and communication technology by small and medium enterprises in Oman: Case of Dhofar region. Journal of Business and Retail Management Research, 11(3), 92–102. http://jbrmr.com/index.php?file=content&id=717

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. J. (2019). Investigating the determinants of employees' cybersecurity behavior: The moderating effect of organizational culture. Computers in Human Behavior, 96, 261–270. https://doi.org/10.1016/j.chb.2019.02.024

Naradda Gamage, S. K., Ekanayake, E. M. S., Abeyrathne, G. A. K. N. J., Prasanna, R. P. I. R., Jayasundara, J. M. S. B., & Rajapakshe, P. S. K. (2020). A review of global challenges and survival strategies of small and medium enterprises (SMEs). Economies, 8(4), 79. https://doi.org/10.3390/economies8040079

Ndungu, S., Wanjau, K., Gichira, R., & Mwangi, W. (2018). Moderating role of entrepreneurial orientation on the relationship between information security risk assessment and firm performance in Kenya. International Journal of Professional Business Review, 3(2), 131–152. https://doi.org/10.26668/businessreview/2018.v3i2.97

Snyman, D., & Kruger, H. (2019). Behavioural threshold analysis: Methodological and practical considerations for applications in information security. Behaviour & Information Technology, 38(11), 1088–1106. https://doi.org/10.1080/0144929X.2019.1584646

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001.