1.

Record Nr.	UNINA9910991163803321
Autore	Palanisamy Rathika
Titolo	Bring Your Own Device Security Policy Compliance Framework / / by Rathika Palanisamy, Azah Anir Norman, Miss Laiha Mat Kiah, Tutut Herawan
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-86801-3
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XXII, 196 p. 26 illus., 13 illus. in color.)
Collana	Information Systems Engineering and Management, , 3004-9598 ; ; 37
Disciplina	620.00285
Soggetti	Engineering - Data processing Data protection Computer security Computer networks - Security measures Data Engineering Data and Information Security Security Services Principles and Models of Security Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Bring Your Own Device -- Theoretical Framework and Hypotheses Development -- Research Methodology -- Analysis, Results and Discussion -- Conclusion and Future Work.
Sommario/riassunto	Proliferation of Bring Your Own Device (BYOD) has instigated a widespread change, fast outpacing the security strategies deployed by organizations. The influx of these devices has created information security challenges within organizations, further exacerbated with employees’ inconsistent adherence with BYOD security policy. To prevent information security breaches, compliance with BYOD security policy and procedures is vital. This book aims to investigate the factors that determine employees' BYOD security policy compliance by using mixed methods approach. Security policy compliance factors, BYOD practices and security risks were identified following a systematic

review approach. Building on Organizational Control Theory, Security Culture and Social Cognitive Theory, a research framework positing a set of plausible factors determining BYOD security policy compliance was developed. Next, with a purposive sample of eight information security experts from selected public sector organizations, interviews and BYOD risk assessments analysis were performed to furnish in-depth insights into BYOD risks, its impact on organizations and recommend control measures to overcome them. This led to the suggestion of four control measures to mitigate critical BYOD security risks such as Security Training and Awareness (SETA), policy, top management commitment and technical countermeasures. The control measures were mapped into the research framework to be tested in the following quantitative phase. The proposed research framework was tested using survey results from 346 employees of three Critical National Information Infrastructure (CNII) agencies. Using Partial Least Squares – Structural Equation Modelling (PLS-SEM), the framework's validity and reliability were evaluated, and hypotheses were tested. Findings show that perceived mandatoriness, self-efficacy and psychological ownership are influential in predicting employees’ BYOD security policy compliance. Specification of security policy is associated with perceived mandatoriness, while BYOD IT support and SETA are significant towards self-efficacy. Unexpectedly, security culture has been found to have no significant relationship to BYOD security policy compliance. Theoretical, practical, and methodological contributions were discussed and suggestions for future research were recommended. The analysis led to a number of insightful findings that contribute to the literature and the management, which are predominantly centered on traditional computing. In view of the ever-increasing BYOD threats to the security of government information, it is imperative that IT managers establish and implement effective policies to protect vital information assets. Consequently, the findings of this study may benefit policymakers, particularly in the public sector, in their efforts to increase BYOD security policy compliance among employees.