DOI: http://dx.doi.org/10.26483/ijarcs.v14i2.6955

ISSN No. 0976-5697

Volume 14, No. 2, March-April 2023

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

FACTORS AFFECTING THE ADOPTION OF SECURE SOFTWARE PRACTICES IN SMALL AND MEDIUM ENTERPRISES THAT BUILD SOFTWARE IN-HOUSE

Wisdom Umeugo
Independent Researcher
Ottawa
Canada

Kimberly Lowrey
Faculty, PhD IT program
School of Computer and Information Sciences
University of the Cumberlands, Kentucky, USA

Shardul Y. Pandya
Professor, Ph.D. IT Program
School of Computer and Information Sciences
University of the Cumberlands, Kentucky, USA

Abstract: Software has grown enormously in value because of its wide use for domestic, public, and economic activities. Software must be secure because exploited software vulnerabilities can negatively affect individuals' and organizations' financial, health, and economic well-being. Various authors recommended practicing a secure software development lifecycle (SSDLC) to ensure that software is released secured. Software small and medium enterprises (SMEs), the dominant software publishers, have not widely adopted the SSDLC. This study approached the problem of software SMEs' inadequate adoption of SSDLC from an innovation adoption perspective based on the diffusion of innovation theoretical framework (DOI). Five DOI factors, relative advantage, compatibility, complexity, trialability, and observability, were assessed for significance to software SMEs' intention to adopt SSDLC. A random sample of 200 participants from a population of software security decision-makers of software SMEs based in the United States that develop software in-house were surveyed via an online close-ended questionnaire. Relative advantage, compatibility, and trialability were statistically significant to SME SSDLC adoption intention. Complexity and observability were not statistically significant to SME SSDLC adoption intention. Trialability was the strongest predictor of SME SSDLC adoption intention. SME software security decision-makers may find that the results of this study help to determine the factors they should consider when deciding to introduce the SSDLC into their software development process. The result of the study has implications for practice and social change because increased SME SSDLC adoption potentially results in the development of more secure software and fewer software security incidents.

Keywords: software security; secure software; secure software development lifecycle; ssdlc; ssdlc adoption; diffusion of innovation

I. INTRODUCTION

Digital transformation is ongoing across economies, bringing unprecedented opportunities for a digital society [1]. Software is a chief enabler of digital transformation [2]. Software applications are widely used across numerous sectors and industries [3]. As a result, the software industry has experienced immense growth [4]. The economic importance of software, its wide deployment, and its use for managing critical daily domestic, social, and economic activities make it invaluable [5]. Software security remains an issue, evidenced by the growing number of reported software vulnerabilities in the National Vulnerability Database. Due to the dominance of SMEs in the software industry, approaches to improve software security must consider software development practices in SMEs [6]. Various literature examining software security processes in organizations have considered traditional software security, which is focused on post-deployment security, to be inadequate, advocating instead for practicing a secure software development lifecycle (SSDLC) [7]–[9]. However, there is insufficient adoption of secure software practices throughout the SDLC, pronounced in SMEs that develop software in-house [10].

Few empirical studies on SSDLC adoption have been published [11]. Existing literature on adopting secure software practices in organizations focuses on individual software developer adoption and acceptance of secure software practices and tools rather than organizational adoption [12]–[14]. According to Jaatun and Cruzes [15], introducing software security practices in SMEs can be considered introducing innovation. For this reason, this research approached the problem of inadequate SME SSDLC adoption from an innovation adoption perspective based on the diffusion of innovation theory (DOI). The objective of this study was to determine the degree of impact of DOI constructs observability, relative advantage, compatibility, trialability, and complexity on software SME intention to adopt SSDLC. This study informs software SMEs' security managers and government policymakers on the critical factors to consider when adopting the SSDLC. The research also fills the existing knowledge gap on the factors affecting the adoption of the SSDLC in software SMEs from an innovation adoption perspective.

II. THEORY AND HYPOTHESIS DEVELOPMENT

This research was concerned with SSDLC adoption at the organizational level. Related studies examining the factors influencing the adoption of secure software development practices in software SMEs focused on the perspectives of software developers, information security professionals, and tools. Woon and Kankanhalli [16] investigated information security (IS) professionals' intention to adopt secure software development practices in the SDLC based on the theory of planned behavior (TPB) and the theory of reasoned action (TRA). Witschey et al. [14] investigated developers' adoption of security tools based on DOI. Deschene [17] performed a Delphi study to determine what would be required to encourage software development stakeholders to adopt secure software practices in the SDLC. Assal and Chiasson [12] interviewed 13 developers recruited from developer forums and social groups on their motivations and amotivations for adopting secure software practices in the SDLC.

Various theoretical frameworks have been used to study information security (IS) and information technology (IT) adoption at the organizational and individual levels. This research focused on the organizational adoption factors influenced by the inherent characteristics of the SSDLC as an innovation. Roger's [18] Diffusion of Innovation theory (DOI) was adopted as the theoretical framework for the research because it considers the impact of the characteristics of innovation on the innovation's adoption. Other theoretical frameworks used to examine technology adoption include the Technology-Organization-Environment (TOE), the Technology Acceptance Model (TAM), the Theory of Planned Behavior (TPB), and the Unified Theory of Acceptance and Use of Technology (UTAUT2).

Rogers' [18] DOI is a popular theory used to describe technology innovation adoption. DOI explains the factors impacting innovation adoption intention, innovation diffusion speed, the innovation adoption process, and the characteristics of innovation adopters [19]. DOI specified five attributes of innovations that impact their adoption: relative advantage, compatibility, complexity, trialability, and observability. These five attributes form the five DOI factors examined in this study as independent variables (IVs) for their relationship to SME SSDLC adoption intention, which is the dependent variable (DV). Fig. 1 shows the relationship between the five DOI factors and SME SSDLC adoption intention.

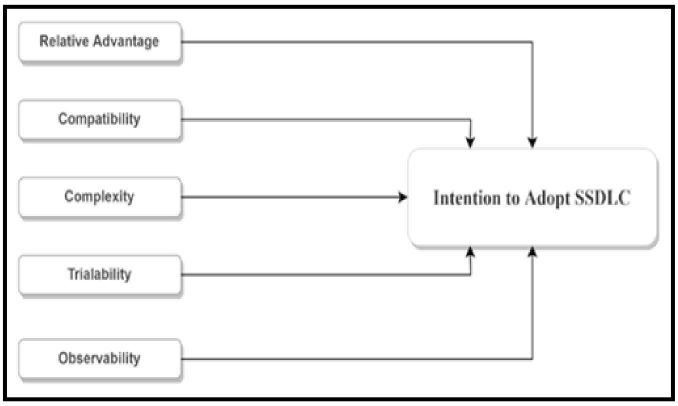

Figure 1. Relationship Between the Independent Variables and the Dependent Variable

A. *Relative Advantage*

Relative advantage (RA) is an innovation's perceived advantages over current solutions [20]. In this study, the relative advantage of the SSDLC is expressed in terms of the increased efficiency of the software security process, improved performance on software security metrics, and overall security of software products. According to Hameed and Arachchilage [20], there should be a positive relationship between RA and IS innovation adoption when the innovation offers more valuable and adequate security. Research Question One was proposed to investigate the significance of relative advantage to SME SSDLC adoption intention.

RQ1: What is the extent to which relative advantage predicts the intention to adopt secure software practices throughout the SDLC in SMEs that develop software in-house?

$H1_0$. There is no statistically significant relationship between relative advantage and the intention to adopt secure software practices throughout the SDLC.

$H1_1$. There is a statistically significant relationship between relative advantage and the intention to adopt secure software practices throughout the SDLC.

B. *Compatibility*

Compatibility (CM) is the consistency and fit of innovation with the organization's existing system, values, and processes [20]. Low levels of innovation compatibility necessitate changes to procedures, cause a considerable effort to learn the innovation and require greater stakeholder commitment to implement the innovation, which can discourage its adoption [21]. Consequently, the greater the compatibility of the IS innovation, the easier it is to adopt [20]. Research Question Two was proposed to investigate the significance of compatibility to SME SSDLC adoption intention.

RQ2: What is the extent to which compatibility predicts the intention to adopt secure software practices throughout the SDLC in SMEs that develop software in-house?

$H2_0$. There is no statistically significant relationship between compatibility and intention to adopt secure software practices throughout the SDLC.

$H2_1$. There is a statistically significant relationship between compatibility and intention to adopt secure software practices throughout the SDLC.

C. *Complexity*

Complexity (CO) is the perceived difficulty in learning and using innovation [20]. The increased complexity of an IS innovation leads to greater implementation difficulty and lower adoption tendency [20]. Therefore, complexity is expected to be negatively correlated with adoption intention. Research Question Three was proposed to investigate the significance of complexity to SME SSDLC adoption intention.

RQ3: What is the extent to which complexity predicts the intention to adopt secure software practices throughout the SDLC in SMEs that develop software in-house?

$H3_0$. There is no statistically significant relationship between complexity and intention to adopt secure software practices throughout the SDLC.

$H3_1$. There is a statistically significant relationship between complexity and intention to adopt secure software practices throughout the SDLC.

D. *Trialability*

Trialability (TR) is an innovation's availability and ability to be experimented with before adoption [20], [22]. According to Hameed and Arachchilage [20], exposure to and experimentation with an innovation increases the potential for its adoption. Research Question Four was proposed to investigate the significance of trialability to SME SSDLC adoption intention.

RQ4: What is the extent to which trialability predicts the intention to adopt secure software practices throughout the SDLC in SMEs that develop software in-house?

$H4_0$. There is no statistically significant relationship between trialability and intention to adopt secure software practices throughout the SDLC.

$H4_1$. There is a statistically significant relationship between trialability and intention to adopt secure software practices throughout the SDLC.

E. Observability

Observability (OB) is the degree of visibility of the results of using the IS innovation to potential adopters [20], [22]. According to Hameed and Arachchilage [20], observability is expected to influence IS innovation adoption positively. Research Question Five was proposed to investigate the significance of observability to SME SSDLC adoption intention.

RQ5: What is the extent to which observability predicts the intention to adopt secure software practices throughout the SDLC in SMEs that develop software in-house?

$H5_0$. There is no statistically significant relationship between observability and intention to adopt secure software practices throughout the SDLC.

$H5_1$. There is a statistically significant relationship between observability and intention to adopt secure software practices throughout the SDLC.

F. SSDLC Adoption intention

In this study, SSDLC adoption intention measures the organization’s propensity and disposition toward adopting the SSDLC. Based on Rogers’ [18] DOI theory, relative advantage, compatibility, complexity, trialability, and observability should all significantly impact the adoption of an innovation. Therefore, the relative advantage, compatibility, complexity, trialability, and observability of SSDLC are expected to have statistically significant relationships with SME SSDLC adoption intention.

III. RESEARCH METHOD

The research was designed to be quantitative non-experimental predictive correlational. The target population for the study was individuals responsible for software security governance and software product security in SMEs that develop software applications in-house in the United States. The typical target roles of the population were staff in software SMEs occupying the position of Chief information officer (CIO), Chief information security officer (CISO), Chief Technology Officer (CTO), Product Manager, Product security manager, Engineering manager, and Tech lead. Members of the desired population were expected to be able to evaluate or make significant contributions to their organization’s decision to adopt secure software practices. The inclusion criteria for the sample frame were (a) the participant should be an adult of age 25 or more; (b) the participant should be currently employed full-time in a software SME based in the United States that develops software in-house; and (c) the participant should be in a role that significantly influences the security governance of their organization’s software products. Members of the population unable or unwilling to give consent were excluded. All Participants were asked screening questions to ensure they passed the inclusion criteria.

A. Sampling

An adequate sample size of 138 was calculated using priori power analysis for multiple linear regression on G*Power 3.1, which was taken as the minimum sample size. The study aimed to have a sample size of 200 or more responses to increase generalizability. Simple random probability sampling was used to ensure an equal chance for the population and increased population generalizability.

B. Instrumentation

The research used an adapted version of the DOI-TOE survey instrument by AlBar and Hoque [23], which already passed reliability and validity tests. The survey instrument was hosted and administered online on Pollfish’s website. The survey instrument was closed-ended, consisting of demographic and five-point Likert-scale questions to test for the variables under study. Pollfish provided the sample frame based on the inclusion and exclusion criteria implemented as filters and screening questions.

C. Statistical Tests

Descriptive statistics were used to describe the participant demographics. The demographic data collected were age, gender, years of experience, and organizational role. The demographics were assessed using totals, frequency, percentage, and mean. Multiple regression analysis was used to evaluate the predictive correlational relationship between the independent and dependent variables. All assumptions of multiple regression were tested before multiple regression analysis was conducted.

IV. RESULTS

The survey was shown to 1,398 respondents, of which 202 met the inclusion criteria by passing the screening questions and providing consent. A total of 200 (n = 200) out of the 202 eligible participants completed the survey. All 200 responses passed quality checks and were retained. The results were exported in CSV format from Pollfish and imported into JASP for statistical analysis. Table I summarizes the participant demographics.

Table I. Participant Demographics

Demographic	**Category**	**Frequency (n)**	**Percent (%)**
Age	25 – 34	88	44.0
	35 – 44	79	39.5
	45 – 54	23	11.5
	54+	10	5
Gender	Female	80	40.0
	Male	120	60.0
Experience	Less than three years	33	16.5
	3 – 5 years	38	19
	6 – 10 years	61	30.5
	11 – 15 years	30	15.0
	16 – 20 years	14	7.0
	20+ years	24	12.0
Organizational role	Owner or Chief Executive Officer (CEO)	25	12.5
	Chief Information Officer (CIO)	25	12.5
	Chief Information Security Officer (CISO)	20	10.0
	Chief Operation Officer	10	5.0
	Chief Technology Officer	37	18.5
	Information Security Manager	18	9.0
	Product Manager	14	7.0
	Tech Lead	15	7.5
	Product Manager	14	7.0
	Software Security Architect	12	6.0
	Other	9	4.5

A. Assumptions Tests

The data were tested for a linear relationship between the DV and all IVs collectively. This was done by constructing and visually examining the plot of standardized residuals vs. predicted values. Fig. 2 shows the plot of standardized residuals vs. predicted values. An even distribution of the residuals around the baseline is visually observable in Fig. 2, satisfying the assumption of linearity.

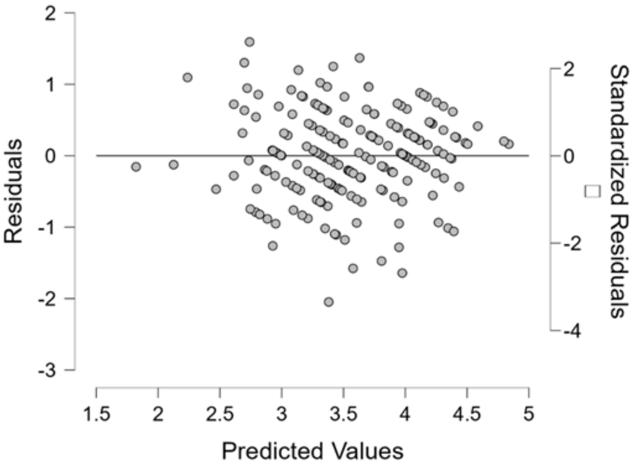

Figure 2. Plot of Residuals vs. Predicted

Homoscedasticity was tested by visually examining the plot of standardized residuals vs. predicted values shown in Fig. 2. There is a visually observable even distribution of residuals around the horizontal line where the residual is 0. No signs of heteroscedasticity are visually observable.

Multicollinearity was tested by calculating the Tolerance and Variance Inflation Factor (VIF) using collinearity statistical data analysis. Table II presents the results of the collinearity statistical analysis. All the IVs had Tolerance values greater than 0.1, indicating that multicollinearity was absent. The calculated Tolerance values satisfied the assumption of no multicollinearity.

Table II. Collinearity Diagnostics

Variable	VIF	Tolerance
Relative Advantage	1.41	0.711
Complexity	1.09	0.921
Compatibility	1.69	0.592
Trialability	1.41	0.707
Observability	1.44	0.695

Outliers and high influential points were identified using casewise diagnostics in JASP. Four cases having ±3 standard deviations were flagged as outliers. All four cases were excluded from the multiple regression analysis, reducing the sample to 196 (N = 196). No cases had Cook's distance greater than 1, indicating no high influential points in the data.

Normality was tested using the Shapiro-Wilk test for normality. A statistic of 0.993 and a p-value of 0.4555 was calculated. The p-value in the Shapiro-Wilk test result was greater than 0.05, indicating normality.

B. *Multiple Regression Analysis*

Multiple regression analysis was conducted on JASP using the enter method. The mean and standard deviation of the scores of each variable were calculated from the values of their composing variables. Table III shows the descriptive statistic for each variable.

Table III. Descriptive Statistics of Variables

Variable	N	Mean	Std. Deviation
Relative Advantage	196	3.412	0.880
Complexity	196	3.223	0.887
Compatibility	196	3.469	0.889
Trialability	196	3.437	0.876
Observability	196	3.459	0.838
Adoption Intention	196	3.558	0.811

A potential regression model, H1, was calculated. R^2 for the model was 43.1%, and adjusted R^2 was 41.6%. The result implied that 43.1% of the variance of IA could be explained by RA, CO, CM, TR, and OB. This model was considered reasonable. Table IV shows the model summary statistics.

Table IV. Model Summary – Adoption Intention

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	0.811
H_1	0.656	0.431	0.416	0.620

ANOVA results in Table. V shows the statistical significance of the proposed model H1. Model H1 was statistically significant (p < 0.001). Therefore, relative advantage, complexity, compatibility, trialability, and observability statistically significantly predicted SSDLC adoption intention, F(190, 5) = 28.762, p < .001, R2 = .431.

Table V. ANOVA Table

Model		Sum of Squares	df	Mean Square		F	p
H_1	Regression	55.197	5	11.039		28.762	< .001
	Residual	72.925	190	0.384			
	Total	128.122	195				

Table VI shows the results of the Coefficients table. Statistical significance (p < 0.05) was observed for relative advantage, compatibility, and trialability. The overall regression model H1 was accepted. The results of the regression model showed that RA was a significant predictor of IA (β = 0.129, t (190) = 1.985, p <.05); CO was not a significant predictor of IA (β = -0.027, t (190) = -0.465, p > .05); CM was a significant predictor of IA (β = 0.272, t (190) = 3.827, p <.001); TR was a significant predictor of IA (β = 0.328, t (190) = 5.043, p <.001); OB was not a significant predictor of IA (β = 0.122, t (190) = 1.864, p >.05). The regression equation for the regression model is as follows.

$$\text{Predicted IA} = 0.916 + 0.119(\text{RA}) - 0.024\,(\text{CO}) + 0.248(\text{CM}) + 0.304(\text{TR}) + 0.118(\text{OB})$$

Table VI. Coefficients Table

Predictor	*B*	Standard Error	β	t	p
(Intercept)	0.916	0.259		3.533	< .001
Relative Advantage	0.119	0.060	0.129	1.985	0.049
Complexity	-0.024	0.052	-0.027	-0.465	0.642
Compatibility	0.248	0.065	0.272	3.827	< .001
Trialability	0.304	0.060	0.328	5.043	< .001
Observability	0.118	0.064	0.122	1.864	0.064

Hypothesis testing was carried out based on the results of the multiple regression analysis. Relative advantage (β = 0.129, t (190) = 1.985, p <.05), compatibility (β = 0.272, t (190) = 3.827, p <.001), and trialability (β = 0.328, t (190) = 5.043, p <.001) were found to be statistically significant predictors of software SME intention to adopt SSDLC. Complexity (β = -0.027, t (190) = -0.465, p > .05) and observability (β = 0.122, t (190) = 1.864, p >.05) were found to not significantly predict IA. Based on the analysis of research questions, the null hypotheses $H1_0$ for relative advantage, $H2_0$ for compatibility, and $H4_0$ for trialability were all rejected in favor of their respective alternative hypotheses $H1_1$, $H2_1$, and $H4_1$. Conversely, the null hypothesis $H3_0$ for complexity and $H5_0$ for observability were failed to reject. Table VII summarizes the results of hypothesis testing.

Table VII. Summary of Hypothesis Testing

Question	Sig	Hypothesis	Result
RQ1	0.049	***H1₀*.** There is no statistically significant relationship between RA and IA.	Rejected
		***H1₁*.** There is a statistically significant relationship between RA and IA.	Supported
RQ2	< .001	***H2₀*.** There is no statistically significant relationship between CM and IA	Rejected
		***H2₁*.** There is a statistically significant relationship between CM and IA.	Supported
RQ3	0.642	***H3₀*.** There is no statistically significant relationship between CO and IA.	Failed to reject
		***H3₁*.** There is a statistically significant relationship between CO and IA.	Unsupported
RQ4	< .001	***H4₀*.** There is no statistically significant relationship between TR and IA.	Rejected
		***H4₁*.** There is a statistically significant relationship between TR and IA.	Supported
RQ5	0.064	***H5₀*.** There is no statistically significant relationship between OB and IA.	Failed to reject
		***H5₁*.** There is a statistically significant relationship between OB and IA.	Unsupported

V. DISCUSSION

Relative advantage was statistically significant and positively correlated to the intention to adopt SSDLC in SMEs that build software in-house. The result confirmed the significance of relative advantage in Rogers' [18] DOI theory. The statistical significance and positive correlation of relative advantage in the research results suggested that software security decision-makers in software SMEs find the SSDLC valuable and acknowledge that adopting the SSDLC will improve the security of their software products. For this reason, efforts to increase software SME SSDLC adoption should raise awareness of the relative advantages of practicing the SSDLC.

Compatibility was determined to be statistically significant and positively correlated to the intention to adopt SSDLC in software SMEs that build software in-house. The analysis confirmed the significance of compatibility in Rogers' [18] DOI theory. The statistical significance and positive correlation of compatibility in the research results suggested that software security decision-makers consider the compatibility of the SSDLC with their existing software practices and values an essential factor in SSDLC adoption. Therefore, efforts to improve software SME SSDLC adoption should promote practicing the SSDLC as an organizational standard and value. Standards and guidelines for incorporating SSDLC into various SDLC models should also be published, particularly for the less popular SDLC models, such as the crystal method, prototyping, and rapid application development.

Complexity was statistically insignificant and negatively correlated to the intention to adopt SSDLC in software SMEs that build in-house software. The statistical insignificance of complexity diverged from Rogers' [18] DOI theory. The reasons for the result are unclear. One explanation for the statistical insignificance of complexity is that software security decision-makers in software SMEs are confident in their organization's ability to implement and incorporate the SSDLC into their existing information security process. Another reason may be that software security decision-makers may not have a complete understanding or experience in implementing the SSDLC. The reasons should be further investigated.

Trialability was determined to be statistically significant and positively correlated to the intention to adopt SSDLC in software SMEs that build software in-house. The result confirmed the significance of trialability in Rogers' [18] DOI theory. Trialability was the most significantly correlated factor in the research results. The statistical significance and positive correlation of trialability in the research results suggested that software security decision-makers consider the practical testing of the SSDLC the most important factor in SSDLC adoption. Therefore, efforts to improve software SME adoption should include practical information on trialing the SSDLC. SSDLC standards and guidelines should consist of easy-to-follow instructions on setting up and trialing the SSDLC in the various SDLC models.

Observability was statistically insignificant and positively correlated to the intention to adopt SSDLC in SMEs that build software in-house. The statistical insignificance of observability diverged from Rogers' [18] DOI theory. The reasons for the result are unclear. One explanation for the statistical insignificance of observability in software SME SSDLC adoption is that software security decision-makers have little visibility into the software security practices of other organizations. However, software security decision-makers acknowledge the relative advantages of practicing the SSDLC. Despite observability's statistical insignificance, its positive correlation to SME SSDLC adoption intention suggested that greater observability might boost SSDLC adoption. For this reason, efforts should be made to encourage software SMEs to share their SSDLC practices and to demonstrate the results of practicing the SSDLC.

VI. LIMITATIONS

This study had several limitations. The first limitation was the narrow scope of the study. The study was aimed at software SMEs based in the United States that produce software in-house. For this reason, results may vary if the same study was conducted with a similar target population in a different country. The second limitation was that the study is limited to software SMEs that develop software in-house. The study did not include factors that affect security decisions for purchased or outsourced software. The third limitation of the study lay in the theoretical model used. The tested theoretical constructs are not the exhaustive set of global factors that impact software SME adoption of SSDLC.

VII. IMPLICATIONS

This study has several theoretical implications. This research demonstrated the application of DOI to adopting practices instead of tools in information security. Among the five DOI factors, complexity and observability diverged from statistical significance contrary to the DOI theory expectation. The research contributed knowledge that filled the existing knowledge gap on the factors considered significant to software SME SSDLC adoption from an innovation standpoint.

There are practical implications for the research. SME software security decision-makers may find that the results of this study help to determine the factors they should consider when deciding to introduce the SSDLC into their software development process. This study provided empirical evidence on the relative advantage, compatibility, complexity, trialability, and observability of SSDLC that organizations can leverage to understand the factors to consider when adopting the SSDLC. The research is also significant to information security policymakers in government. Software controls critical public infrastructure, making it the target for malicious state actors. Therefore, the government needs to foster the security of the software used for public infrastructure. The results of this research can help the government make a case for SSDLC adoption in SMEs, particularly those software SMEs that are government software contractors. The study's results can also help guide government information security policy by informing policymakers on the significant predictors of SSDLC adoption in software SMEs.

VIII. CONCLUSION

Software must be built securely from the early stages of its lifecycle. Efforts must be made to improve SME adoption of the SSDLC. Increased software security helps improve safety, assurance, and trust in public infrastructure run by software. The research approached the research problem from an innovation adoption perspective to provide software security decision-makers with the factors they should consider necessary in their decisions to adopt SSDLC. The study contributed to the knowledge of information security adoption, specifically to the adoption of software security practices. Information security and software security decision-makers looking to adopt the SSDLC are recommended to prioritize SSDLC's relative advantage, compatibility, and trialability in their consideration. Information security policymakers in government can make a case for SSDLC adoption in SMEs by promoting its relative advantages and fostering research on techniques and frameworks to improve compatibility and easy trialing of the SSDLC.

IX. FUTURE RESEARCH

There are various opportunities for future research. The reasons for the statistical insignificance of complexity and compatibility should be investigated using qualitative research methods. Qualitative case studies and phenomenology studies should be conducted to explore the SSDLC adoption process in software SMEs to provide rich practical information, recommendations, and frameworks to help software security decision-makers trial and implement the SSDLC. Software SMEs will likely adopt the SSDLC if they find it compatible with their SDLC practices. Therefore, future studies can explore and model the application of the SSDLC across SDLC models, including the less popular SDLC models such as the crystal method, the big bang model, extreme programming, prototyping, and rapid application development. Future studies should also replicate this study across similar populations in various countries to increase the generalization of the results. The scope of this study was also limited to in-house software development. There is an opportunity for future research to extend the study to software security practices for outsourced and purchased software.

X. REFERENCES

[1] OECD, OECD skills outlook 2019: thriving in a digital world. OECD, 2019.

[2] N. Yusupova and K. Mironov, "Key information technologies for digital economy.," Proceedings of REMS 2018 Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT, vol. 2254, p. 330, 2018.

[3] S. R. Sree and C. P. Rao, "A study on application of soft computing techniques for software effort estimation," in A Journey Towards Bio-inspired Techniques in Software Engineering, vol. 185, J. Singh, S. Bilgaiyan, B. S. P. Mishra, and S. Dehuri, Eds. Cham: Springer International Publishing, 2020, pp. 141–165.

[4] Gartner, "Gartner Forecasts Worldwide IT Spending to Reach $4.4 Trillion in 2022," Gartner, May 06, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-04-06-gartner-forecasts-worldwide-it-spending-to-reach-4-point-four-trillion-in-2022 (accessed May 15, 2022).

[5] J. Ransome and A. Misra, Core Software Security. Auerbach Publications, 2018.

[6] M. Tuape and Y. Ayalew, "Factors affecting development process in small software companies," in 2019 IEEE/ACM Symposium on Software Engineering in Africa (SEiA), May 2019, pp. 16–23, doi: 10.1109/SEiA.2019.00011.

[7] H. Al-Matouq, S. Mahmood, M. Alshayeb, and M. Niazi, "A maturity model for secure software design: A multivocal study," IEEE Access, vol. 8, pp. 215758–215776, 2020, doi: 10.1109/ACCESS.2020.3040220.

[8] R. Fujdiak et al., "Managing the secure software development," in 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Jun. 2019, pp. 1–4, doi: 10.1109/NTMS.2019.8763845.

[9] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic mapping study on security approaches in secure software engineering," IEEE Access, vol. 9, pp. 19139–19160, 2021, doi: 10.1109/ACCESS.2021.3052311.

[10] F. Alghamdi, "Motivational company's characteristics to secure software," in 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Mar. 2020, pp. 1–5, doi: 10.1109/ICCAIS48893.2020.9096815.

[11] E. Venson, R. Alfayez, M. M. F. Gomes, R. M. C. Figueiredo, and B. Boehm, "The impact of software security practices on development effort: an initial survey," in 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Sep. 2019, pp. 1–12, doi: 10.1109/ESEM.2019.8870153.

[12] H. Assal and S. Chiasson, "Motivations and amotivations for software security.," SOUPS Workshop on Security

Information Workers (WSIW). USENIX Association, p. 1, 2018.

[13] Z. A. Maher, A. Shah, S. Chandio, H. M. Mohadis, and N. H. B. A. Rahim, "Challenges and limitations in secure software development adoption - A qualitative analysis in Malaysian software industry prospect," IJST, vol. 13, no. 26, pp. 2601–2608, Jul. 2020, doi: 10.17485/IJST/v13i26.848.

[14] J. Witschey, O. Zielinska, A. Welk, E. Murphy-Hill, C. Mayhorn, and T. Zimmermann, "Quantifying developers' adoption of security tools," in Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering - ESEC/FSE 2015, New York, New York, USA, Aug. 2015, pp. 260–271, doi: 10.1145/2786805.2786816.

[15] M. G. Jaatun and D. Soares Cruzes, "Care and feeding of your security champion," in 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Jun. 2021, pp. 1–7, doi: 10.1109/CyberSA52016.2021.9478254.

[16] I. M. Y. Woon and A. Kankanhalli, "Investigation of IS professionals' intention to practise secure development of applications," Int. J. Hum. Comput. Stud., vol. 65, no. 1, pp. 29–41, Jan. 2007, doi: 10.1016/j.ijhcs.2006.08.003.

[17] M. Deschene, "Embracing security in all phases of the software development life cycle: A Delphi study," Undergraduate thesis, 2016.

[18] E. M. Rogers, "Diffusion of innovations/everett m. rogers.," NY: Simon and Schuster, vol. 576, 2003.

[19] S.-H. Hwang, J.-H. Lee, and Y. Hu, "Diffusion and adoption of smart media in china," APJCRI, vol. 7, no. 12, pp. 67–77, Dec. 2021, doi: 10.47116/apjcri.2021.12.07.

[20] M. A. Hameed and N. A. G. Arachchilage, "A conceptual model for the organizational adoption of information system security innovations," in Security, privacy, and forensics issues in big data, R. C. Joshi and B. B. Gupta, Eds. IGI Global, 2020, pp. 317–339.

[21] T. Lynn, X. Liang, A. Gourinovitch, J. Morrison, G. Fox, and P. Rosati, "Understanding the determinants of cloud computing adoption for high performance computing," presented at the Hawaii International Conference on System Sciences, 2018, doi: 10.24251/HICSS.2018.489.

[22] J. Kaminski, "Diffusion of innovation theory.," Canadian Journal of Nursing Informatics, vol. 6, no. 2, pp. 1–6, 2011.

[23] A. M. AlBar and Md. R. Hoque, "Factors affecting cloud ERP adoption in Saudi Arabia: An empirical study," Information Development, vol. 35, no. 1, pp. 150–164, Jan. 2019, doi: 10.1177/0266666917735677.