The Role of Cybersecurity on SME's Digital Finance Adoption

Sri Mangesti Rahayu[1], Saparila Worokinasih[2*], Cacik Rut Damayanti[3], Yudha Alief Aprilian[4], Rani Arifah Normawati[5]
*saparila.fia@ub.ac.id
ORCID: 0000-0001-6950-9954

Universitas Brawijaya, Indonesia[1,2,3,4]
Akademi Komunitas Negeri Putra Sang Fajar, Indonesia[5]

Abstract. Implementing digital transformation is very important for Small and Medium Enterprises (SMEs) to enhance competitiveness and productivity. Therefore, it is essential to identify the role of cybersecurity awareness and preparedness in SMEs' digital finance adoption. This study examines the impact of cybersecurity awareness and preparedness on SMEs' digital finance adoption using a Structural Equation Model (SEM). The research was conducted on 185 SMEs in East Java, Indonesia. The findings suggest that cybersecurity awareness and preparedness positively and significantly affect digital finance adoption. These results contribute to understanding SMEs' cybersecurity and digital finance adoption. Digital financial adoption can directly enhance financial inclusion. However, digital transformation efforts must be accompanied by cultivating cybersecurity awareness.

Keywords: cybersecurity awareness, cybersecurity preparedness, digital finance adoption

1. Introduction

Modern-day society is driven by technology [1]. The industrial revolution and digital transformation have changed human lives, both at the individual level, professional activities, and the social environment [2], [3], [4]. Digital technology, created and adopted by humans, offers convenience, benefits, and vast economic and social opportunities. Still, on the other hand, it brings new risks and vulnerabilities that cannot be ignored. One of these risks is the threat of cybercrime [2], [1].

Currently, cybercrime threats are not only targeting individuals but also organizations [1]. Organizations are seen to have significant resources that cybercriminals can exploit. Cybercrime can have negative impacts on an organization's performance, not only financially but also overall organizational performance [5]. Cybersecurity within an organization is a challenge that must be met to secure the resources and assets owned by the organization. Therefore, investment in cybersecurity is also considered a crucial factor in organizational sustainability.

For large organizations, investment in cybersecurity has been around for a while. Many large organizations have invested in this area, and in 2022, cybersecurity became the top expenditure area for organizations. Data from the Enterprise Strategy Group (ESG) shows that 69% of organizations plan to spend more on cybersecurity in 2022. Another 29% stated that cybersecurity spending would remain roughly the same as in 2021, and only 2% of organizations intended to pay less for cybersecurity in 2022 compared to 2021 [6].

This phenomenon differs for Small and Medium-sized Enterprises (SMEs), especially in Indonesia. SMEs in Indonesia are at the beginning of their digital transformation journey. The

AICOBPA 2023, November 01, Malang, Indonesia

DOI 10.4108/eai.1-11-2023.2355313

COVID-19 pandemic acted as a catalyst and accelerated the digital transformation of SMEs. The digital transformation of SMEs is being driven from various angles, including by the government through digital onboarding programs [7]. In this digital onboarding program, several activities have transformed towards digital adoption, including adopting digital finance for SME business operations. This is considered strategic because changes in economic and business patterns in society can provide a new space for recovery from the pandemic's challenges and create more significant opportunities for SMEs to grow.

Amid this migration and adoption process, cybersecurity for SMEs has become a crucial issue. SMEs are considered vulnerable to cyber threats [2] and are now becoming targets of cyberattacks [1]. According to statistics from 2020 by Fundera, as much as 43% of cybercrimes were targeted at SMEs [8]. Meanwhile, a survey conducted by ESET 2022 stated that the most significant negative impacts of cybercrime are data loss, financial losses, loss of consumer trust, operational disruptions, and damage to reputation [9]. This aligns with the opinions of experts that cybercrime can impact business continuity, intellectual property, personal and professional integrity [2], financial losses, the loss of customers or business partners, a decrease in the firm's market value, and damage to the firm's reputation [10].

This risk certainly disrupts the sustainability of SMEs. The threat of cybercrime is a real challenge for SMEs. However, the majority of SMEs believe that their organizations will not face cybersecurity risks and do not understand the significant impact that can result from these threats [2],[11]. Most SMEs will only invest in cybersecurity after experiencing the real impact of cybercrimes [12].

Preparing for cybersecurity amid the adoption of digital technology is a challenge for SMEs. This is because of the lack of awareness, insufficient resources, and expertise related to cybersecurity issues in SMEs [1]. The limited visibility and public awareness of cybersecurity are the most significant challenges to address [10]. The limited resources and knowledge SMEs possess are why they need to know what preventive actions to take to address cyber threats [2], [13]. Preparing cybersecurity measures can significantly impact the overall company's performance [5]. Meanwhile, cybersecurity preparedness must be done, as digitalization cannot be avoided while cybersecurity risks evolve dynamically. Therefore, achieving cybersecurity is not a destination but an ongoing journey. Cybersecurity awareness [1] is required for SMEs to understand that cybersecurity is a business function that can support their sustainability.

Based on the background, it is essential to evaluate the influence of cybersecurity awareness on cybersecurity preparedness for establishing cybersecurity in SMEs, especially concerning digital finance adoption. This evaluation is based on the Hierarchy of Effects Model, where awareness is followed by usage. The proposed constructs form a model to determine how cybersecurity awareness and cybersecurity preparedness in SMEs have progressed and contributed to SMEs' digital finance adoption overall. The unity of this model is an asset in developing digital entrepreneurship in Indonesia and enhancing financial inclusion through the adoption of digital finance.

2. Literature Review

2.1. Hierarchy of Effects Model

The Hierarchy of Effects Model refers to the stages that influence consumer decisions. The Hierarchy of Effects Model is based on a theory developed by Gray A. Steiner and Robert J. Lavidge in 1961. The original theory outlines the stages of the consumer's purchasing or product usage decision-making process, starting with awareness, knowledge, liking, preference, and convictions and concluding with purchase/usage [14]. This model is a foundation for developing various research models, such as the Awareness, Attitude, Usage (AAU) Model or Awareness, Trust, Usage (ATU) Studied.

2.2. Cyber Security

Cybersecurity can be defined as a set of processes, governance, management, tools, policies, and controls used to secure the digital environment. This includes assets (such as information and virtual assets), entities (such as end-users, organizations, governments, communities, machines, and software), and interactions to eliminate, reduce, or mitigate the risks of unauthorized access, control, disruption, or other cyberattacks [15]. Cybersecurity is the practice of protecting computers, systems, and networks from both internal and external threats. It is also known as information technology security or electronic information security, focusing on keeping software and devices free from hazards [10].

The primary function of cybersecurity is to safeguard the devices we use and the services we access from theft or damage, including preventing unauthorized access to a large amount of personal information. Given the importance of cybersecurity, organizations consider it a fundamental pillar in their business decision-making [16]. Organizations and public policymakers in various countries are also increasingly concerned about this critical issue [15]. Types of cyber threats include cybercrime, cyber-attacks, and cyberterrorism. Common methods to threaten cybersecurity include malware, SQL injection, phishing, man-in-the-middle attacks, and denial-of-service attacks [17].

2.3. Digital Finance

Digital finance refers to using digital technology, such as mobile devices and the Internet, to enable and enhance financial performance. Digital Finance can improve financial inclusion by making financial services more accessible and affordable for underserved populations. It can also improve the efficiency and security of financial transactions, reduce costs, and increase transparency. In the business domain, digital technology must evolve with business logic so that business and its management can integrate into digitalization [18]. This is crucial to ensure that individuals or organizations can optimistically access digital business and financial processes using digital technology [19]. In this research, digital finance refers to an organization's entire digital-based financial system, including basic access to financial services, sending and receiving money through e-money, e-commerce, budgeting, e-accounting, and other digital financial services for financing [20].

3. Methodology

This research examined the influence of cybersecurity awareness and preparedness on developing digital finance adoption. This study is explanatory research with a quantitative approach to test the relationships between variables. The primary data was collected by an online survey and direct interviews. From 185 respondents who completed the questionnaire, we used Partial Least Square analysis to answer whether the hypotheses were accepted or rejected. This tool is powerful with a small number of samples as well as to predict the mediating effects of the relationship [6].

3.1. Research Concept

This research framework is based on the Hierarchy of Effects Model developed by Gray A. Steiner and Robert J. Lavidge in 1961 [31]. Gray and Lavidge [31] stated that the use of something begins with awareness, knowledge, liking, preference, and convictions. These three aspects are divided into three categories: cognitive, affective, and conative.

In this study, the proposed research concept model adopts and simplifies this model. It is explained in the Hierarchy of Effects Model that the stages of an individual's decision-making process start from the cognitive aspect to the conative aspect [14]. The cognitive aspect can be in the form of awareness. This research is represented by cybersecurity awareness. The conative aspect represents the tendency to take action, described in this study by cybersecurity preparedness and digital finance adoption. The process of adopting the theory into this research can be seen in the following diagram:

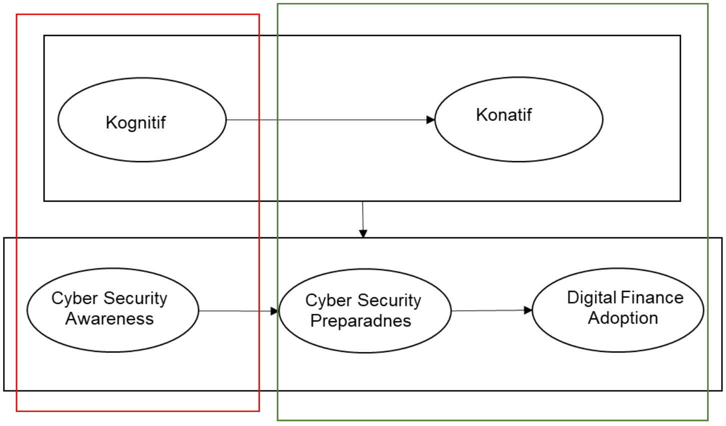

Figure 1: Research concept model

3.2. Hypothesis Model

[21] examined the influence of security awareness on security preparedness in Small and Medium Enterprises (SMEs). Saban stated that with the increasing importance of security, awareness, and commitment to information security, SME executives' perception of security preparedness also increases. When SME executives perceive the importance of protecting their business from security threats and are more aware and committed to information security, they believe their business should be better prepared to mitigate security threats [11].

Renaud Ophoff researched 361 SMEs in the UK. The results showed that SMEs' cyber situational awareness influences cybersecurity controls and precautions. Renaud & Ophoff's research showed that the influence test on both variables resulted in positive path coefficients with a p-value < 0.05. Based on this, the hypothesis proposed is:

H1: Cybersecurity awareness significantly affects cybersecurity preparedness.

In the Hierarchy of Effects Model, someone's awareness of something will be followed by a motive to implement it; in other words, awareness will be followed by different stages and lead to the decision "to use" or the "usage" stage. Empirically, [20] stated that national cyber security commitment positively affects business usage. In other studies, [22] tested user awareness's influence on adopting digital financial services. Other studies show the relationship of awareness to the utilization of online digital tools, as the results of [23] indicate. Further research testing the influence of awareness on usage is widely conducted in different fields, such as healthcare [24], [25], [26]. The hypothesis proposed is:

H2: Cybersecurity awareness significantly affects the adoption of digital finance.

The conative aspect in the Hierarchy of Effects Model includes several stages, represented in this study by preparedness and adoption. [30] studied the relationship between preparedness and adoption. In their research, Sani stated that readiness affects adoption. Another study by [27] examined the cybersecurity readiness variable on the organizational security adoption variable. Based on this, the hypothesis proposed is:

H3: Cybersecurity preparedness significantly affects digital finance adoption.

In the Hierarchy of Effects Model, how individuals respond to a message or something is explained by a series of stages followed by individuals taking action. The first stage is awareness, which is a cognitive aspect. The conative aspect follows it, or the motive to take a specific activity or the decision to take action. Referring to this, the hypothesis proposed is:

H4: Cybersecurity awareness significantly affects digital finance adoption through cybersecurity preparedness.

The proposed hypothesis model can be seen in the following diagram:

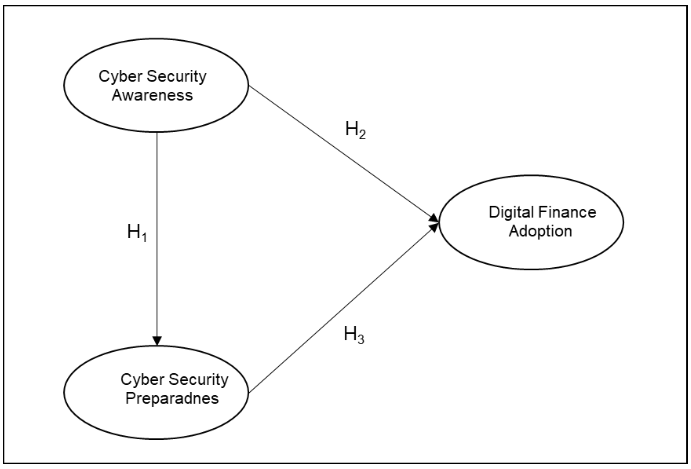

Figure 2: Research hypothesis model

3.3. Operational Definition of Variables

An operational definition is an implementation guide for measuring a variable. The following is the Operational Definition of Variables table for this research:

Table 1: Operational definition of variables

Variable	Item	Reference
Cyber Security Awareness	1) Awareness of cybersecurity practices 2) Awareness of cybersecurity threats 3) Organizational commitment 4) Information about cybersecurity	[11] [13]
Cyber Security Preparedness	1) Implementation of security policies 2) Cybersecurity team 3) Cybersecurity policies and procedures 4) Training and education 5) Access restrictions	[11] [13]
Digital Finance Adoption	1) Basic access to financial services 2) Money transfer and payments	[20].

	3) E-commerce trade/utility bill 4) Budgeting and financial planning 5) Borrowing and Insurance	

Source: Data compiled by researchers, 2023

4. Result and Discussion

The respondents of this research are MSMEs in East Java Province. Respondents were obtained through survey methods distributed through online media and survey platforms and by visiting respondents directly to validate the answers given. In this data collection, 216 respondents participated, and 185 completed the questionnaire.

The criteria for the research population are having a business domicile in East Java and using digital financial technology for business operations. The digital finance criteria refer to Khrisna et al.'s (2022) (24) research. The characteristics of respondents in using digital finance are that the majority of respondents, around 35%, use a combination of money transfers and payments and use marketplaces or e-commerce. About 25% revealed that they used money transfers and payments. Meanwhile, 12% of respondents had used all four criteria.

Characteristics of respondents based on business sector include trade, processing industry, fisheries, plantations, animal husbandry, agriculture, and services. Most respondents have been in business for 0 to 5 years, 77%. This category often reflects self-employment, which may have started as a small business or a growing hobby. As many as 8% of respondents were in the 6 to 7-year category, which can be interpreted as businesses with moderate or limited growth. This number may include businesses that already exist but have yet to reach a significant growth stage or may have reached their growth limits. Meanwhile, around 15% of respondents have businesses over seven years old, which reflects a competitive and well-established business. The business length category is based on the categories presented by [28]. The characteristics of the number of employees owned by respondents in this study provide an overview of the size of the business represented by respondents based on BPS criteria. Most respondents (66%) represent micro-businesses with 1-4 employees, around 25% of respondents represent small businesses with 5-19 employees, and medium businesses with 20-99 employees are only represented by 9% of the total respondents.

Table 2: Characteristics of respondent

Description	Frequency	Percentage
Digital Finance Use		
✓ money transfer and payments	46	25%
✓ marketplace or e-commerce	6	3%
✓ money transfer and payments ✓ marketplace or e-commerce	65	35%
✓ money transfer and payments ✓ budgeting or e-accounting application	9	5%
✓ money transfer and payments ✓ borrowing and Insurance	5	3%
✓ marketplace and e-commerce ✓ budgeting or e-accounting application	1	1%
✓ money transfer and payments ✓ marketplace or e-commerce	17	9%

Description	Frequency	Percentage
✓ budgeting or e-accounting application		
✓ money transfer and payments ✓ marketplace or e-commerce ✓ borrowing and insurance	12	6%
✓ money transfer and payment ✓ budgeting or e-accounting application ✓ borrowing and Insurance	1	1%
✓ money transfer and payments ✓ marketplace or e-commerce ✓ budgeting or e-accounting application ✓ borrowing and insurance	23	12%
Total	185	100%
Business Longevity		
0 - 5 years	143	77%
6 - 7 years	15	8%
> 7 years	27	15%
Total	185	100%
Number of Employees		
1-4	122	66%
5-19	47	25%
20-99	16	9%
Total	185	100%

Source: Data compiled by researchers (2023)

The hypothesis proposed in this research was tested using inferential statistics after several stages of data analysis. In this research, inferential data analysis was measured using Partial Least Square-Structural Equation Modeling (PLS-SEM), which was carried out to test the relationship between variables and to explore or confirm theories in explanatory research [29].

The validity testing procedure is carried out by correlating item scores with the construct score, producing a loading factor value. A variable is declared valid if the loading factor is positive and greater than 0.5. Based on running data, one indicator was obtained with a loading factor value <0.5, so it had to be removed (Y2.5) (Table 3).

Table 3: Results of loading factor testing

Variable and Indicator		1st Perform SEM Analysis		2nd Perform SEM Analysis		3rd Perform SEM Analysis	
		Loading Factor*	P Value	Loading Factor*	P Value	Loading Factor*	P Value
Cyber Security Awareness	$X_{1.1}$	0.764	<0.001	0.764	<0.001	<0.001	<0.001
	$X_{1.2}$	0.820	<0.001	0.820	<0.001	0.820	<0.001
	$X_{1.3}$	0.865	<0.001	0.865	<0.001	0.865	<0.001
	$X_{1.4}$	0.786	<0.001	0.786	<0.001	0.786	<0.001

Cyber Security Preparedness	$Y_{1.1}$	0.705	<0.001	0.705	<0.001	0.705	<0.001
	$Y_{1.2}$	0.776	<0.001	0.776	<0.001	0.776	<0.001
	$Y_{1.3}$	0.814	<0.001	0.814	<0.001	0.814	<0.001
	$Y_{1.4}$	0.783	<0.001	0.783	<0.001	0.783	<0.001
	$Y_{1.5}$	0.561	<0.001	0.560	<0.001	0.560	<0.001
Digital Finance Adoption	$Y_{2.1}$	0.624	<0.001	0.734	<0.001	0.830	<0.001
	$Y_{2.2}$	0.638	<0.001	0.730	<0.001	0.796	<0.001
	$Y_{2.3}$	0.683	<0.001	0.676	<0.001	0.607	<0.001
	$Y_{2.4}$	0.722	<0.001	0.613	<0.001	Removed	
	$Y_{2.5}$	0.499	<0.001	Removed			

*Positive loading factor value and > 0.5: Valid
Source: Data processed by researchers (2023)

Additionally, an assessment of the value of the Square Root of Average Variance Extracted (AVE) for each construct was conducted. An instrument meets the convergent validity test with an Average Variance Extracted (AVE) above 0.5. Based on the initial test results, there was a variable with an AVE value of 0.5 (Y2). If AVE values do not meet the criteria, it is possible to eliminate indicators, specifically those with the most minor loading factor. Since Y2.5 is the indicator with the minor loading factor and does not meet the validity test criteria using the loading factor, this indicator must be removed from the constructed model.

In the second test, an AVE value was obtained that still does not meet the criteria (>0.5), so the indicator with the most minor loading factor must be removed (Y2.4). The removal of this indicator can be done if there are still other indicators representing the variable. The AVE results can be seen in Table 4.

Table 4: Average variance extracted (AVE)

Variable	AVE*		
	1st Perform SEM Analysis	**2ndPerform SEM Analysis**	**3rd Perform SEM Analysis**
Cyber Security Awareness	0.656	0.656	0.656
Cyber Security Preparedness	0.538	0.538	0.538
Digital Finance Adoption	0.407	0.476	0.564

*AVE value > 0.5: Valid
Source: data processed by researchers (2023)

Discriminant validity is calculated using cross-loading with the criteria that if the loading factor value is greater than the correlation between the indicator and other variables, the indicator is considered valid in measuring the corresponding variable. Cross-loading factor values can be found in Table 5.

Table 5: Cross loading

Item	X_1*	Y_1*	Y_2*
X_{11}	**0.764**	-0.085	-0.045
X_{12}	**0.820**	-0.276	0.122
X_{13}	**0.865**	-0.009	0.061
X_{14}	**0.786**	0.381	-0.150

Y_{11}	0.210	**0.705**	-0.055
Y_{12}	-0.228	**0.776**	-0.108
Y_{13}	-0.275	**0.814**	-0.007
Y_{14}	-0.011	**0.783**	0.013
Y_{15}	0.467	**0.560**	0.211
Y_{21}	0.166	-0.091	**0.830**
Y_{22}	-0.039	-0.203	**0.796**
Y_{23}	-0.176	0.390	**0.607**

*Loading factor value is greater than the correlation between the indicator and other variables
Source: Data processed by researchers (2023)

Calculations that can be used to test construct reliability are composite reliability and Cronbach's alpha. The test criteria state that the construct is declared reliable if the composite reliability is greater than 0.7. On the other hand, if Cronbach's Alpha is greater than 0.6, then the construct is expressed as reliable.

Table 6: Composite reliability and Cronbach's alpha

Variable	Composite Reliability*	Cronbach's Alpha**
Cyber security awareness (X)	0.884	0.824
Cyber security preparedness (Y_1)	0.851	0.780
Digital finance adoption (Y_2)	0.792	0.605

*Composite reliability ≥0.7
**Cronbach’s Alpha ≥ 0,6: Reliable
Source: Data processed by researchers (2023)

After going through the validity and reliability testing stages to obtain valid and reliable results, testing the direct and indirect influence of the Path was carried out with the following results:

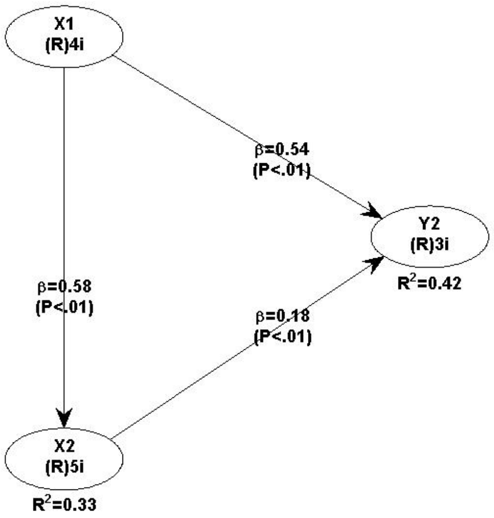

Figure 3: Path diagram

Table 7: Research hypothesis testing result

Exogenous	Intervening	Endogenous	Path Coeff*	SE	P Values**
Cyber Security Awareness	-	Cyber Security Preparedness	0.576	0.066	<0.001
Cyber Security Awareness	-	Digital Finance Adoption	0.542	0.066	<0.001
Cyber Security Preparedness	-	Digital Finance Adoption	0.178	0.071	0.007
Cyber Security Awareness	Cyber Security Preparedness	Digital Finance Adoption	0.102	0.051	0,003

*path coefficient - : negative influence ; path coefficient +: positive influence
**p-value ≤ level of significance (alpha = 5%)
Source: Data processed by researchers (2023)

4.1. Cyber Security Awareness on Cyber Security Preparedness

Based on the direct influence test, the first hypothesis of this study is accepted. The Path Coefficient results are 0.576, SE: 0.066, P-Value: <0.001, indicating that cyber security awareness positively and significantly affects cyber security preparedness. The test results show that cyber security awareness influences cyber security preparedness, as reflected by its four indicators. This means that the higher the cyber security awareness one possesses, the better their cyber security preparedness tends to be. Conversely, someone with negative cyber security awareness will likely have poor cyber security preparedness.

The positive influence of cyber security awareness on cyber security preparedness supports the Hierarchy of Effects Model, which forms the basis for this hypothesis. As the Hierarchy of

Effects Model explains, an individual's decision-making process starts with cognitive aspects and ends with conative aspects [14]. Awareness can represent cognitive aspects, as in this study's representation of cyber security awareness. Meanwhile, conative aspects represent the tendency to take action, represented by cyber security preparedness in this study.

Empirically, the findings of this study align with research conducted by Saban et al. (2021) [11], which explored the influence of security awareness on security preparedness in Small and Medium Enterprises (SMEs). Saban stated that as the importance of security, awareness, and commitment to information security increases, SME executives' perception of security readiness also improves. When SME executives perceive the importance of protecting their businesses from security threats and are more aware and committed to information security, they believe their businesses must be better prepared to mitigate security threats [11].

The findings of this study also reinforce the results of Renaud & Ophoff (2021) [13]. Renaud Ophoff researched 361 SMEs in the UK, and their results showed that SMEs' cyber situational awareness affects cyber security controls and precautions.

4.2. Cyber Security Awareness on Digital Finance Adoption

The test results on the influence of cyber security awareness on digital finance adoption show a Path Coefficient of 0.542, SE: 0.066, P-value: <0.001. This means that cyber security awareness positively and significantly impacts the adoption of digital finance. Therefore, the second hypothesis is accepted. This can be interpreted as follows: the higher one's cyber security awareness is, the more likely they are to adopt digital finance. Conversely, if someone has low cyber security awareness, it is less likely to be followed by digital finance adoption.

Theoretical findings from the test results on cyber security awareness and digital finance adoption variables support the Hierarchy of Effects Model. An individual with awareness of something is followed by the motive to implement it. In the Hierarchy of Effects Model, awareness is followed by other stages, ultimately leading to the decision "to use" or the "usage" stage.

Empirically, the results of this study align with the research conducted by [20], where national cyber security commitment positively impacts business usage. These findings also support the research undertaken by [22], which examined the influence of user awareness on the adoption of digital financial services. Other studies have shown the relationship between awareness and the utilization of online digital tools, as demonstrated in the research by [23].

4.3. Cyber Security Preparedness on Digital Finance Adoption

The test results on the influence of cyber security preparedness on digital finance adoption yield a Path Coefficient of 0.178, SE: 0.071, P-Value: 0.007. This indicates that cyber security preparedness positively and significantly influences digital finance adoption. Therefore, the third hypothesis in this study is accepted. This relationship shows that the level of preparedness in dealing with cyber security threats also has a significant positive influence on digital finance adoption. However, this influence is lower than cyber security awareness's impact on digital finance adoption.

In the Hierarchy of Effects Model, the conative aspect includes several stages, which in this study are represented by preparedness and adoption. The influence of both variables in this study shows a significant positive effect, indicating that preparedness leads to adoption. Theoretically, these findings can support the model Gray A Steiner and Robert J Lavidge proposed. Furthermore, empirically, the influence of preparedness on adoption supports the research conducted by [30], who studied IT adoption in SMEs. In their study, Sani stated that readiness has an impact on adoption. Additionally, the results of this study support the research by [27], where the variable of cyber security readiness has a significant positive effect and a strong relationship with the variable of organizational security adoption.

4.4. Cyber Security Awareness on Digital Finance Adoption through Cyber Security Preparedness

The test of the mediating effect between cyber security awareness and digital finance adoption through cyber security preparedness yields a Path Coefficient of 0.102, SE: 0.051, P-Value: 0.003. These results indicate a positive and significant influence, where cyber security preparedness can mediate the relationship between cyber security awareness and digital finance adoption. In this mediating relationship, cyber security preparedness provides partial mediation. This means that whether or not there is cyber security preparedness, it still positively and significantly influences the relationship between cyber security awareness and digital finance adoption. However, when comparing the direct and indirect effects, it becomes evident that this mediating variable reduces the direct impact of cyber security awareness on digital finance adoption.

5. Conclusion and Implication

The results of this research have both theoretical and practical implications. The theoretical implications provide evidence that awareness affects preparedness and preparedness affects adoption or usage, in line with the Hierarchy of Effects Model. Empirically, this study demonstrates that cybersecurity awareness impacts cybersecurity preparedness and influences digital finance adoption, including using money transfers and payments, marketplace and e-commerce, budgeting or e-accounting applications, and digital finance for borrowing and insurance. The findings in this research can support, reinforce, or even weaken the findings of previous studies.

The implications for policymakers and practitioners are that the research findings can be used to determine policy directions in cyber security and financial inclusion, which can be achieved through digital financial adoption. Specifically, the managerial implications signal that cybersecurity awareness is important for shaping cybersecurity preparedness. Both cybersecurity awareness and cybersecurity preparedness can serve as strong points for the development of digital financial adoption. Conversely, to enhance digital financial adoption among SMEs, it is necessary to increase their awareness of the importance of cybersecurity when using this technology.

Digital financial adoption can directly enhance financial inclusion. However, digital transformation efforts must be accompanied by cultivating cybersecurity awareness. This step ensures that SMEs have a strong foundation when implementing digital technology in their businesses and minimize the risks arising during the digital transformation. Achieving cybersecurity is not the endpoint but a continuous journey. Cybersecurity awareness is a shared responsibility among the public, private, and individuals. Support for cybersecurity for SMEs needs to be provided. The government, in turn, is responsible for creating a conducive environment for the digital transformation of SMEs, implementing policies that promote cybersecurity, striving for improved cyber skills, and ensuring the security of information exchange. Given the primary constraint of limited resources, startups with financial service products should also participate in this ecosystem. Promoting digital finance products must include education, best practices, and campaigns about protecting personal, financial, and business data. However, regardless of the government's support through various mechanisms or the private sector's moral attention, the issue of cybercrime is a personal responsibility for SMEs.

This research certainly has limitations. One of the limitations identified is the partial application of the Hierarchy of Effects Model, focusing only on how awareness can influence preparedness, thereby impacting adoption. Therefore, further research should adopt the model entirely to obtain a broader picture of how the Hierarchy of Effects Model can be applied in the adoption of digital technology. In addition, this study is limited to specific areas, encompassing the population of SMEs. This means the findings may not fully reflect situations or behaviors that differ in different regions or contexts. Therefore, the research findings may only apply to regions or populations similar to the ones studied.

References

[1] Bada M, Nurse JRC. Developing cybersecurity education and awareness programs for small- and medium-sized enterprises (SMEs). Information and Computer Security. 2019;27(3):393–410.

[2] Kertysova K. Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. The European Economic and Social Committee. 2018. 76–85 p.

[3] Alzubaidi A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon. 2021;7(1).

[4] Autio E, Fu K, Smit W, Muftiadi A, Chiyachantana C, Prasarnphanich P, et al. Adoption of digital technologies , business model innovation , and financial and sustainability performance in startup firms. 2022;1–46.

[5] Hasan S, Ali M, Kurnia S, Thurasamy R. Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications. 2021;58.

[6] Drew Robb. 2022 cybersecurity spending trends: Where are organizations investing? [Internet]. INFOSEC. 2022 [cited 2023 Mar 5]. Available from: https://resources.infosecinstitute.com/topics/industry-insights/it-spending-trends/

[7] KEMEMKOPUKM. SIARAN PERS KEMENKOPUKM [Internet]. 2021 [cited 2023 Feb 5]. Available from: https://kemenkopukm.go.id/read/ri-kejar-30-juta-umkm-go-digital-hingga-2024

[8] Fundera. Pentingnya Keamanan Siber Bagi 10,2 Juta Pelaku UMKM di Jagat Digital. 2020;1–3.

[9] Ancaman Siber UKM Meningkat [Internet]. PROSPERITA IT NEWS. 2022 [cited 2023 Feb 28]. Available from: https://news.prosperita.co.id/ancaman-siber-ukm-meningkat/

[10] Foya D. Assessing Cyber Security Awareness and organisational preparedness on cyber security in audit firms The case of the big 4 audit firms EY Deloitte KPMG PWC 2017 2020 (1). International Journal of Scientific & Engineering Research. 2022;13(3).

[11] Saban KA, Rau S, Wood CA. “SME executives’ perceptions and the information security preparedness model”. Information and Computer Security. 2021;29(2):263–82.

[12] ESET. ESET releases new SMB research, finds businesses lose hundreds of thousands of euros in data security breaches [Internet]. 2022 [cited 2023 Mar 1]. Available from: https://www.eset.com/int/about/newsroom/press-releases/company/eset-releases-new-smb-research-finds-businesses-lose-hundreds-of-thousands-of-euros-in-data-securit/

[13] Renaud K, Ophoff J. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Process and People. 2021;1(1):24–46.

[14] Chakravarty R, Sarma NN. Evolutionary framework of hierarchy of effects models: exploring relevance in the shifting of customer path. Vilakshan - XIMB Journal of Management. 2022;19(1):59–68.

[15] Dedeke A, Masterson K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. Information and Computer Security. 2019;27(3):373–92.

[16] Rabii A, Assoul S, Ouazzani Touhami K, Roudies O. Information and cyber security maturity models: a systematic literature review. Information and Computer Security. 2020;28(4):627–44.

[17] Kaspersky. What is Cyber Security? [Internet]. [cited 2023 Feb 5]. Available from: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[18] Hanafizadeh P, Kim S. Digital Business: A new forum for discussion and debate on digital business model and digital transformation. Digital Business. 2020;1(1):1–2.

[19] Pinto SO, Sobreiro VA. Literature review: Anomaly detection approaches on digital business financial systems. Digital Business. 2022;2(2):100038.

[20] Krishna B, Krishnan S, Sebastian MP. Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective. Information Systems Frontiers. 2022;(0123456789).

[21] Saban K, Rau S, Wood C. “SME executives’ perceptions and the information security preparedness model”. Information & Computer Security. 2021 Mar 29;ahead-of-print.

[22] Anane I, Nie F. Determinants Factors of Digital Financial Services Adoption and Usage Level: Empirical Evidence from Ghana. International Journal of Management Technology. 2022;9(1):26–47.

[23] Alordiah CO, Osagiede MA, Omumu FC, Okokoyo IE, Emiko-Agbajor HT, Chenube O, et al. Awareness, knowledge, and utilisation of online digital tools for literature review in educational research. Heliyon. 2023;9(1):e12669.

[24] SUN CX, HE B, MU D, LI PL, ZHAO HT, LI ZL, et al. Public Awareness and Mask Usage during the COVID-19 Epidemic: A Survey by China CDC New Media. Biomedical and Environmental Sciences. 2020;33(8):639–45.

[25] Rahman Zuthi MF, Hossen MA, Pal SK, Mazumder MH, Hasan SMF, Hoque MM. Evaluating knowledge, awareness and associated water usage towards hand hygiene practices influenced by the current COVID-19 pandemic in Bangladesh. Groundwater for Sustainable Development. 2022;19(November 2021):100848.

[26] Downes JM, Appeddu LA, Johnson JL, Haywood KS, James BJ, Wingard KD. An exploratory survey on the awareness and usage of clinical practice guidelines among clinical pharmacists. Exploratory Research in Clinical and Social Pharmacy. 2021;2:100013.

[27] Berlilana, Noparumpa T, Ruangkanjanases A, Hariguna T, Sarmini. Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. Sustainability (Switzerland). 2021;13(24).

[28] Tewari PS, Skilling D, Kumar P, Wu Z. Competitive Small and Medium Enterprises A diagnostic to help design smart SME policy About this document. 2013.

[29] Ketchen DJ. A Primer on Partial Least Squares Structural Equation Modeling. Vol. 46, SAGE. California: SAGE Publications Inc.; 2013. 184–185 p.

[30] Sani A, Rahman TKA, Budiyantara A, Doharma R. Measurement of readiness in IT adoption among SMEs manufacturing industry in Jakarta. Journal of Physics: Conference Series. 2020;1511(1):0–9.

[31] Lavidge RJ and Steiner GA, “A model for predictive measurements of advertising effectiveness,” *Journal of Marketing*, vol. 25, pp. 59–62, Oct. 1961.