Li Falah-Jurnal Studi Ekonomi Dan Bisnis Islam
Volume 4 (No.2 2019)53-73
P-ISSN: 2541-6545, E-ISSN: 2549-6085

Li Falah
Journal of Islamic Economics and Business Studies
journal homepage: http://ejournal.iainkendari.ac.id/lifalah

Cybersecurity Awareness and Digital Skills on Readiness For Change in Digital Banking

Mun Yah Zahiroh
UIN Sunan Kalijaga, Yogyakarta, Indonesia
e-cmail: munyah.zahir@gmail.com

ARTICLE INFO

Article History:
Received November 8, 2020
Received in revised form November 30, 2020
Available online December 31, 2020

Keywords:
Cybersecurity Awareness; Digital Skills; Change Readiness; Digital Banking, Islamic Banking Human Resources

http://dx.doi.org/10.31332/lifalah.v5i2.2271

A B S T R A C T

This study will explore the impact of cybersecurity awareness and digital skills on readiness for digital banking change. The study sample is fresh graduates in Indonesia's Islamic Banking. The study used PLS-SEM (Partial Least Squares-Structural Equation Modeling) using Smart-PLS 3.0 software. Research shows that 1) cybersecurity awareness does not impact digital banking readiness for change. 2) digital skills have a positive and essential effect on digital banking readiness for change. This study's implications are expected to facilitate the Islamic Banking department in Indonesia to develop its curriculum by including digital intelligence in the Merdeka Belajar curriculum.

1. Introduction

The Covid-19 pandemic changes everything. Governments have implemented various policies related to physical distancing in multiple parts of the world. The guidelines change the pattern of people's activities. Most community activities must be carried out from home and online to break the Covid-19 chain. This finding has led to "work from home" and "study from home" being implemented in the process. Various policies from home encourage the rapid use of the internet in society. As of January 2020, Indonesia's number of internet users has reached 175.4 million, an increase of 17% from January 2019 (Hootsuite and We Are Social 2020), then an increase of 10% until April 2020 (Kementerian Komunikasi dan Informatika RI 2020). The increasing number of internet uses also drives an upward trend for cybercrime. The National Cyber and Crypto Agency (BSSN) noted that during the Covid-19 pandemic, January 1 to April 12, 2020, cybercrime had reached 88,414,296 cases (Kompas.com 2020).

As cybercrime increases, every organization must establish policies to maintain and improve their information technology (Sumin, 2016). Data from the I.T. company, Kaspersky antivirus maker, shows that during the Covid-19 pandemic period, January-May 2020, 40.5 million phishing attacks had occurred on the world's banking business sector (CNN Indonesia 2020). Phishing is a type of malware where someone tries to steal the personal information data of other people (victims) by sending fake emails (Vayansky and Kumar 2018). Furthermore, Kaspersky's data shows that hackers carried out cyber attacks on the banking system through phishing by sending fake emails to bank employees or officials. Phishing will be successful if the targeted employees or bank officials open the link in the email; personal and company data can be stolen. Malware can be installed on the company computer used to access the email. This information shows that cybersecurity awareness is a must among banking employees, including Islamic banking.

Before the pandemic hit globally, the issue of *fintech* that would shift banking's role had already been discussed by many experts. The presence of *fintech* and technology business actors like this has been a challenge for the banking industry in recent years. The banking industry must also compete with the technology industry with such rapid transformation (Wirjoatmodjo, 2018). Banking transformation and digitization must be carefully designed, from preparing infrastructure and human resources (H.R.) to qualified policymakers' regulations (Satria 2018). Based on data from the 2019-2024 Sharia Economic Master Plan issued by the National Committee for Islamic Economics and Finance, the quantity and quality of human resources (H.R.) of Islamic banks in Indonesia are inadequate, B.U.S. information technology has not been able to support Islamic bank service products, and the quality is below conventional bank technology. The development of *fintech*, if not utilized properly, will threaten the development of the Islamic banking industry (Komite Nasional Keuangan Syariah 2018).

In their research, Gasser et al. (2017) from Harvard estimate that by 2025, the banking industry's value chain starting from customer behavior, banking operations, banking revenue acceptance models, big data, and platforms banking, will completely transform into digital banking. The Covid-19 pandemic will undoubtedly accelerate this change because people's internet usage behavior increases. Islamic banking human resources must keep up with these changes and correct deficiencies in quality. Adopting technology requires adequate digital skills. In 2019, Indonesia was ranked 14th as the country with the lowest level of digital technology use than several other countries, especially those in the ASEAN region, such as Singapore, which was ranked first. Even though internet use behavior among Indonesians has

increased during the pandemic, data from 2019 shows that digital skills in Indonesia are still low compared to other ASEAN countries.

From the description above, a crucial issue related to the quality of the human resources of Islamic banking raises, especially on the level of cybersecurity awareness and digital skills of the human resources in Islamic banking in Indonesia, whether cybersecurity awareness and digital skills will affect their Readiness for Change in digital banking. This research will measure cybersecurity awareness and digital skills of fresh graduates majoring in Islamic Banking in Indonesia during the Covid-19 pandemic because this pandemic is a time of very large-scale technology transformation, and new Islamic Banking graduates must have a competitive edge in seeking employment. In the banking sector, at a time of contracted economic growth. The research results are quite important as an evaluation for the Islamic banking department in Indonesia.

2. Literature Review

2.1 Cybersecurity Awareness

Cybersecurity awareness is 1) the level of understanding of internet users about the importance of information security; 2) the responsibilities and actions of internet users to implement information security controls efficiently to protect the organization's data and networks (Shaw et al., 2009). Cybersecurity awareness refers to the ability to identify possible threats to cyberspace, assess the dangers, and prevent or solve problems in cyberspace promptly to protect personal data and property security(Wang et al., 2019). Committee on National Security Systems (CNSS) provides a shorter definition of cybersecurity awareness, namely the ability to protect or defend internet use from cyber attacks (Teer, Kruck, and Kruck 2007). It is possible to infer from these concepts that awareness of cybersecurity is the level of awareness among Internet users of the possibility of manipulating internet information and the control to ensure that crimes do not occur on the internet.

2.2 Digital Skills

NUI Galway (2020) defines digital skills are a set of digital technology skills, including computers and computer applications, tablets and *smartphones*, websites, online platforms, and many more. The expansion of the digital economy and an increasingly digitalized society around the world requires people today to be equipped with a range of digital skills that will enable them to succeed in their work and daily life because they can take advantage of more opportunities in the advancement of digital technology (International Telecommunication Union (I.T.U.) 2018).

According to Van Deursen & Van Dijk (2009), four types of digital skills include: 1) Operational skills, namely skills to operate digital media; 2) Formal skills, namely skills in handling unique structures in digital media such as website menus and hyperlinks; 3) Information skills, namely the skills to find, select and evaluate information in digital media; 4) Strategic skills, namely the skills to use the information contained in digital media as a means to achieve specific personal or professional goals.

2.3 *Change* Readiness

Readiness for change is a derivative variable of Change Management and Organizational Development, a study of Human Resource Management. Readiness for change is the beliefs, attitudes, and intentions of organizational members about the extent to which changes are needed by the organization and the administrative capabilities of the organization's capacity to make these changes succeed (Achilles A. Armenakis, Stanley G. Harris, and Kevin W. Mossholder 1993). A more recent definition of change readiness is how employees perceive the need for organizational change positively and believe that such changes are likely to positively impact their broader implications for the organization (Jones 2005). Readiness for change will gain success if each employee or individual organization has the belief that: 1) they can implement the proposed changes (changing self-efficacy); 2) the proposed changes are appropriate for the organization (conformity); 3) leaders committed to the proposed change (management support), and 4) proposed changes benefit organizational members (Holt et al. 2007).

2.4 Digital Banking

Otoritas Jasa Keuangan or the Financial Service Authority (2016) defines digital banking as services or activities using electronic or digital means belonging to the Bank and or through digital media belonging to prospective customers and or Bank customers, which are carried out independently. Digital banking enables prospective customers and or Bank customers to obtain information, communicate, register, open accounts, banking transactions, and close accounts, including obtaining other information and transactions outside of banking products, including financial advice, investment, electronic-based trading system transactions (*e-commerce*), and different needs of Bank customers.

Due to the rapid development of information technology, digitalization has changed the financial services industry, including banking. This development allows new business processes and leads to entirely new business models, and even shows a radical change in the entire banking value chain as value chains in other changing industries such as the media industry (Ito, Narula, and Ali 2017). Gasser et al., (2017) in their research entitled *Digital*

Banking 2025; the banking industry will transform into six areas: 1) Banking customers 2025: A decrease in the number of physical customer services and use of e-*banking* intensive forces many banks to adapt to new customer service process to maintain contact with customers. Interaction with customers and between companies can be carried out through various digital channels such as applications, social media, to video chat; 2) The banking operational model in 2025: the current banking organizational structure tends to be vertical, in the future there will be a lot of automation of banking value chains, a lot of human labor is replaced by machines so that the organizational structure tends to be decentralized; 3) The banking revenue model 2025: Declining market share through increasingly fierce competition with other banks and *fintech* of non-bank, low-interest-rate environment, increased fees as a result of regulatory requirements, all have led to lower bank profitability. The development of a new digital ecosystem allows banks to reposition themselves in the banking value chain, as well as other value chains, and develop new revenue models such as collaboration with technology-based companies and innovative service providers; 4) digital banking platform in 2025: Generation Y customer era, characterized by an increase in electronic customer services and cross-company transaction processing services that will integrate customers, banks and third-party service providers through *a* platform of new digital banking; 5) Data-based banking 2025: *Big data* is a support service related to customer information, especially new customers. Data allows banks to get a complete view of customers and offer new services according to customer preferences. For example, customer shopping transaction data can become *big data* about what customers consume most. This information can become data on customer preferences; 6) Banking value chain 2025: In recent years, many *fintech* of non-bank entered the banking value chain. For example, technology companies such as Apple (ApplePay) or Google (Google Wallet) sever direct transaction relationships between consumers and banks by providing their electronic money services directly to consumers and only using banks as transaction processing providers. Other examples are bankless service providers such as Wealthfront or Nutmeg for investment or *peer-to-peer* lending in financing (online loans). These new developments indicate a shift towards new banking value chains and compel banks to rethink their current business models radically

2.5 The *Relationship* between Cybersecurity Awareness and Change Readiness in Digital Banking.

Ernest & Young, in a 2015 survey, found that employees who are careless and less aware are the top vulnerability factors that concern companies (Muhirwe and White 2016). Students who lack cybersecurity awareness and enter the workforce threaten recruiting companies; students as prospective employees who are prepared to join the crew must have cybersecurity awareness (Teer, Kruck, and Kruck 2007). Mapoka et al. (2019), in their research titled "*Hack the Bank and Best Practices for Secure Bank*," concluded that to maintain banking's digital security, a bank employee needs an awareness routine about cyber theft. From this description, the first hypothesis that can be formed is:

> H1: *Cybersecurity Awareness* has a positive and significant effect on Change Readiness in *Digital Banking*

2.6 2.6. The Relationship between Digital Skills and Change Readiness in Digital Banking

Digital banking is a radical change in the entire banking business value chain (Ito, Narula, and Ali, 2017). Good change management is needed in the transition period in digital banking. Change management is essential, enabling people to accept new processes, technologies, systems, structures, and values. It is a series of activities that help people move from their current way of working to how they want to work (Ryerson 2011). Digital skills are fundamental to consider, especially in a relatively fast-changing work environment (International Telecommunication Union (I.T.U.) 2018). Digitalization in banking makes the banking business relatively fast-changing. People with more digital skills can take advantage of more opportunities generated with changing advances in digital technology, platforms, and devices. People with relevant digital skills can safely access news and information, communicate online, access essential services related to e-health, e-government, digital finance, agriculture, smart transportation, and otherwise enjoy the many benefits of participating in a globalized world (International Telecommunication Union (I.T.U.) 2018). The second hypothesis is as follows:

H2: *Digital Skills* have a positive and significant effect on Change Readiness in *Digital Banking*

3. Research Method

From the time dimension, this research includes cross-section research, which is only conducted once and represents a specific period in time (Cooper and Schindler 2014). The purposive sampling technique took the sample in this study. Purposive sampling is a sampling technique by basing specific characteristics (Sekaran, 2011). The features of the sample in this study are fresh graduates majoring in Islamic Banking in 2020. In this study, new graduates

are the ready-to-work force and graduated during a period of radical changes in technology adoption due to the pandemic and contraction of economic growth. It is assumed to have adequate technological readiness efforts. According to Roscoe (1975) cited in Sekaran (2011), a sample size of more than 30 and less than 500 is appropriate for most studies. This study consisted of 101 fresh graduates majoring in Islamic Banking from PTKIN-PTKIN and PTS-PTS in Indonesia. It was in the birth range of 1994-2000, generations Y (millennial) and Z.

In this study, three variables will be studied, namely *Cybersecurity Awareness* (X1), *Digital Skills* (X2), and Change Readiness in *Digital Banking* (Y). Each variable will be measured by a questionnaire from experts with a Likert scale of 1-5. The following is a table of variable operations in this research:

Table 1. Operational Variable

Variables	Questionnaire	Indicators	Question Number Item	Scale
Cybersecurity Awareness (X1) is a latent variable exogenous	*Cybersecurity Awareness Survey* (C.A.S.) is arranged Peker et al. (2016)	CSA1, CSA2, CSA3, CSA4, CSA5, CSA6, CSA7, CSA8, CSA9, CSA10, CSA11, CSA12, CSA13, CSA14, CSA15, CSA16, CSA17, CSA18, CSA19	19	Likert 1-5
Digital Skills (X2) are latent variables exogenous	*Digital Skills of Dutch Citizens* compiled by Van Deursen & Van Dijk (2009)	1) *Operational skills* (operational skills): DS1.1, DS1.2, DS1.3, DS1.4, DS1.5, DS1.6, DS1 .7, DS1.8, DS1.9, DS1.10, DS1.11, DS1.12 2) *Formal skills* (formal skills): DS2.1, DS2.2, DS2.3, DS2.4 3) *Information skills* (information skills): DS3.1, DS3.2, DS3.3, DS3.4 4) *Strategic skills*: DS4.1, DS4.2, DS4.3, DS4.4	24	Likert 1-5
Readiness Changed in *Digital Banking* (Y) is an endogenous latent variable of	*Readiness for Change* compiled by Bouckenooghe et al. (2009) by adding object *Digital Banking*	1) *Emotional readiness for change* : KBDB1.1, KBDB1.2, KBDB1.3, KBDB1.4, KBDB1.5 2) *Cognitive readiness for change* : KBDB2.1, KBDB2.2, KBDB2.3, KBDB2.4, KBDB2.5 , KBDB2.6 3) *Intentional readiness for change* : KBDB3.1, KBDB3.2, KBDB3.3, KBDB3.4	15	Likert 1-5

Source: Processed Data, 2020

The study analysis uses PLS-SEM (*Partial Least Squares -Structural Equation Modeling*) using the program *software Smart*-PLS 3.0. P.L.S. (*Partial Least Squares)* is S.E.M. (*Structural Equation Modeling*). S.E.M. is a statistical technique that can analyze the relationship between latent variables and their indicators, latent variables with one another, and direct measurement errors. It allows analysis between several dependent (endogenous) and independent (exogenous) variables directly (J. F. J. Hair et al. 2006). According to Wold (1985), as cited in Ghozali & Latan (2015). P.L.S. is a powerful analysis method and is often called soft modeling because it eliminates O.L.S. (Ordinary Least Squares) regression. Such data must be normally distributed *multivariate*, and there is no multicollinearity problem between exogenous variables. Besides, SEM-PLS is a popular research analysis used for current research and does not require many samples (J. F. Hair et al. 2019), so these assumptions are suitable for this study.

PLS-SEM analysis consists of two sub-models, namely, evaluating the measurement model (*outer model*) and then evaluating the structural model (*inner model*). Evaluation of the measurement model (*external model*) shows how the manifested or observed variable represents the latent variable to be measured. In contrast, the structural model (*inner model*) shows the estimation strength between latent and construct variables (Ghozali and Latan 2015). The following is the equation of the measurement model (*outer model*) and structural model (*inner model*) according to Ghozali & Latan (2015) :

a. Measurement Model (*outer model*)
   The measurement model *outer model*) in this study is a reflective measurement model, which is a test to produce values such as *loading*, *Cronbach's alpha*, *composite reliability*, AVE, HTMT (J. F. Hair et al. 2019), which is the result value. Validity and Reliability Test. The equation for the *outer model* reflective can be written as follows:
   $x = \lambda_x \xi + \varepsilon_x$
   $y = \lambda_y \eta + \varepsilon_y$
   Where:
   - X is a manifest variable or indicator for the exogenous latent construct (ξ), and y is a variable or indicator for the endogenous latent construct (η).
   - And is a loading matrix that describes a simple regression coefficient that connects latent variables and their indicators.
   - and is a residual measurement error (*measurement error*)

b. Structural Model (*inner model*)
   The structural model (*inner model*) will produce values such as R-Square, Significance, and Model fit (J. F. Hair et al. 2019). The equation for the structural model (*inner model*) can be written as follows:
   $\eta = \beta_0 + \beta\eta + \Gamma\xi + \zeta$
   Where η represents the latent variable's dependent vector, ξ describes the independent vector of the latent variable, and ζ refers to the residual variable vector. Because P.L.S. is designed for a recursive model, the relationship between latent variables, each latent

dependent variable (endogenous) η or called the *causal chain system* of latent variables can be specified as follows:

$$\eta_j = \sum_i \beta_{ji} \eta_i + \sum_i \gamma_{jb} \xi_b + \zeta_j$$

In which $\beta_{ji}\gamma_{ji}$ and is the path coefficient that connects the endogenous predictors and the exogenous latent variables ξ and η along with the index range i and b, and ζ_j is the *inner residual variable*.

The following is the research model design in this study with *Cybersecurity Awareness* as an exogenous latent variable (X1), *Digital Skills* as an exogenous latent variable (X2), and Change Readiness in *Digital Banking* as an endogenous latent variable (Y):

.

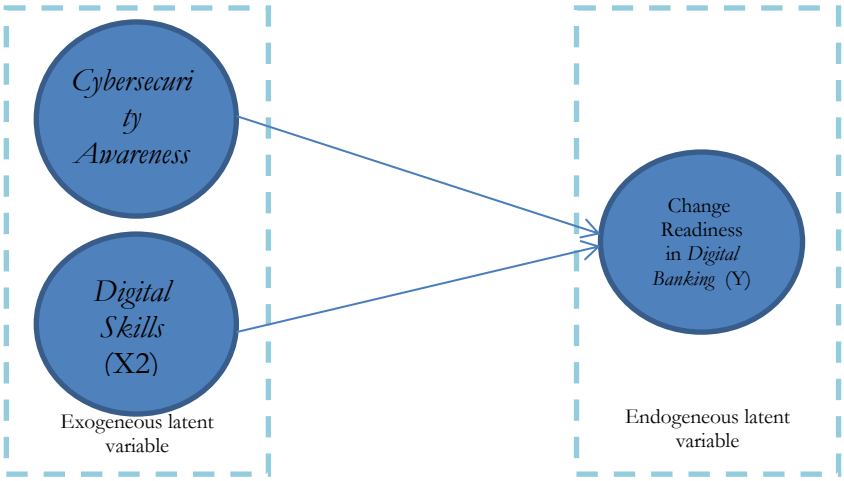

Figure 1: Research Model Design
Source: Processed Data, 2020

4. Result and Discussions

4.1 Result

4.1.1 Evaluation of Measurement Model (*Outer Model*)

The evaluation of the measurement model (*outer model*) consists of two stages: the validity test and the reliability test. In this study, the measurement model (*external model*) is reflective. The validity test consists of the convergent and discriminant validity tests (J. F. Hair et al. 2019).

a. Validity Test

- Convergent Validity Test

Convergent validity test is the extent to which variants of the indicator question items can explain or measure the latent variables' constructs (J.F. Hair et al. 2019). Convergent validity test will be evaluated with value *loading* and AVE (*Average Variance Extracted*).

The standard loading factor value that can be accepted is ≥ 0,5 dan more acceptable if the value is ≥ 0,7 (J. F. J. Hair et al. 2006). In this research, the indicator question items were

declared valid value of *the loading factor is* ≥ 0,6. The following are the results of the loading value of the latent variable question items for convergent validity testing through the software program called Smart-PLS 3.0:

Table 2. Output Value of Loadings Indicator Latent

Cybersecurity Awareness (C.S.A.) X1		Digital Skills (D.S.) X2		Change Readiness in Islamic Banking (KBDB) Y	
Question Item X1	Loading Value 2	Question Item X2	Loading Value	Question Item Y	Loading value
CSA1	0,505	DS1.1	0,560	KBDB1.1	0,675
CSA2	0,180	DS1.2	0,453	KBDB1.2	0,505
CSA3	0,286	DS1.3	0,450	KBDB1.3	0,746
CSA4	0,563	DS1.4	0,683	KBDB1.4	0,771
CSA5	0,460	DS1.5	0,485	KBDB1.5	0,748
CSA6	0,596	DS1.6	0,486	KBDB2.1	0,755
CSA7	0,477	DS1.7	0,603	KBDB2.2	0,712
CSA8	0,579	DS1.8	0,739	KBDB2.3	0,754
CSA9	0,342	DS1.9	0,783	KBDB2.4	0,627
CSA10	0,266	DS1.10	0,590	KBDB2.5	0,886
CSA11	0,572	DS1.11	0,773	KBDB3.1	0,716
CSA12	0,557	DS1.12	0,766	KBDB3.2	0,659
CSA13	0,530	DS2.1	0,766	KBDB3.3	0,773
CSA14	0,600	DS2.2	0,630		
CSA15	0,636	DS2.3	0,766		
CSA16	0,523	DS2.4	0,839		
CSA17	0,637	DS3.1	0,689		
CSA18	0,611	DS3.2	0,593		
CSA19	0,404	DS3.3	0,569		
		DS3.4	0,609		
		DS4.1	0,400		
		DS4.2	0,636		
		DS4.3	0,717		
		DS4.4	0,501		

Source: processed data, 2020

There are 15 questions for the latent variable *cybersecurity awareness* (C.S.A.), which are declared invalid because the loading value is ≤ 0.6, and 4 questions are declared valid. In the latent variable *digital skills* (D.S.), there are six invalid questions (loading value ≤ 0.6) out of 12 questions on the operational skills indicator, all questions on the traditional skills indicator are declared valid (loading value ≥ 0.6), 2 Invalid question items (loading value ≤ 0.6) out of 4 question items on the information skills indicator, and two invalid questions (loading value ≤ 0.6) out of 4 questions on the strategic skills indicator. For the latent variable Readiness for Change in digital banking (KBDB), there is an invalid question item (loading value ≤ 0.6) out

of 5 questions on the indicator of emotional Readiness for Change, while all the questions are on the indicator of cognitive Readiness for Change and intentional Readiness for Change is declared valid (loading value ≥ 0.6). The invalid data were then reduced and tested again, resulting in indicator questions declared valid with loading values ≥ 0.6. Here is an overview of the results:

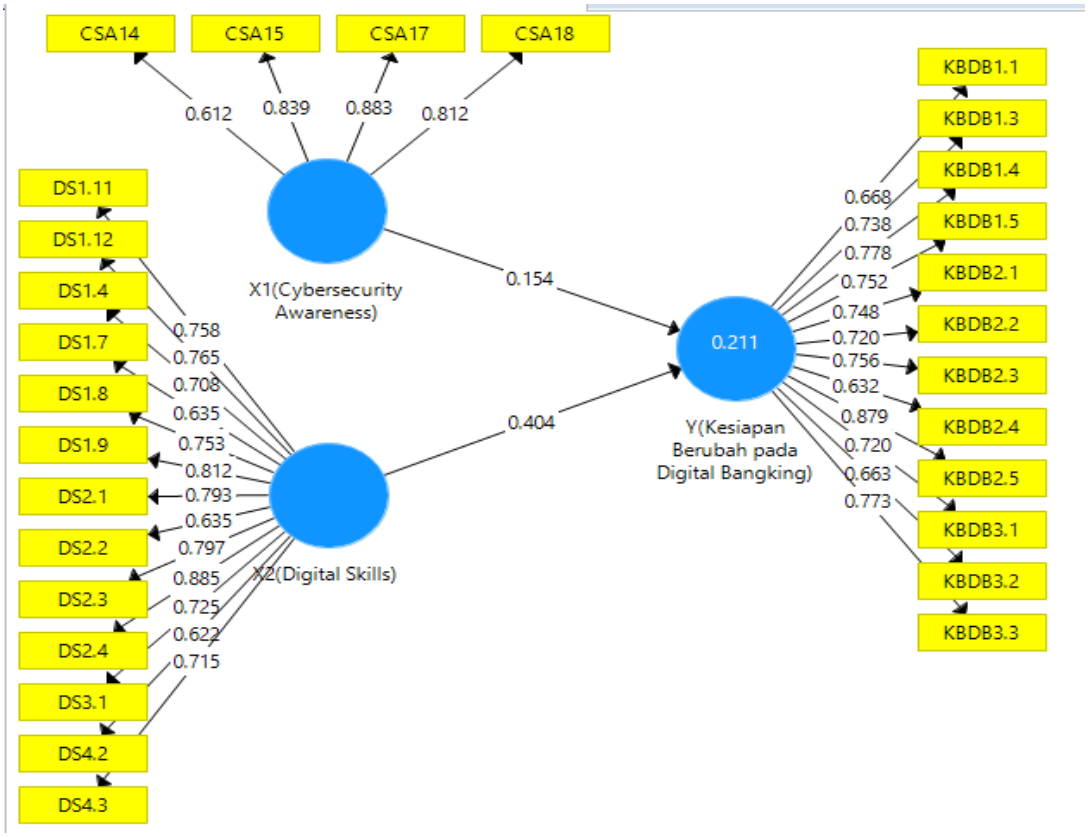

Figure 2. Output Value of Loadings *for* Latent Variable Indicators After Reduction
Source: Processed Data, Tahun 2020

The figure above shows the second test results, and all indicator questions are declared valid with a loading value of ≥ 0.6.

The next test for convergent validity is the AVE test. Latent variables are declared valid if the AVE value is ≥ 0.5 (J.F. Hair et al. 2019). All latent variables in this study were declared valid because the AVE value was ≥ 0.5. Following are the test results:

Table 3. *Average Variance Extracted* (AVE) Result

Variable	AVE	Description
Cybersecurity Awareness (X1)	0,629	Valid
Digital Skills (X2)	0,551	Valid
Change Readiness (Y)	0,545	Valid

Source: Processed Data, 2020

- Discriminant Validity Test

The discriminant validity test is the extent to which a latent variable construct is empirically different from other latent variable constructs in a structural model (J. F. Hair et al. 2019). The discriminant validity test will test the *Fornell Larcker Criterion* and *Cross Loadings values.* A latent variable is declared valid if the correlation value *Fornell Larcker Criterion* between the latent variable and the latent variable itself is higher than the correlation value between the latent variable and other latent variables (Ghozali and Latan 2015). Latent variable correlation value *cybersecurity awareness* with latent variables *cybersecurity awareness* alone is 0.793, higher than the latent variable correlation with *digital skills* (0.198) and readiness to change on *digital banking* (0.234). Likewise, for the latent variable of *digital skills* and Readiness for Change in *digital banking,* the latent variable's correlation value is higher than the other latent variables. Following are the test results:

Table 4. Results of *Fornell Larcker Criterion*

Variable	*Cybersecurity Awareness* (X1)	*Digital Skills* (X2	Change Readiness (Y)	**Description**
Cybersecurity Awareness (X1)	0,793			Valid
Digital Skills (X2)	0,198	0,742		Valid
Change Readiness in Digital Banking (Y)	0,234	0,434	0,738	Valid

Source: Processed Data, 2020

The latent variable indicator question items are declared valid if the correlation value of *cross-loadings* between the latent variable indicator questions and the latent variable itself is higher than the latent variable indicator question items with other latent variables. The results of *cross-loadings of* all indicator question items are declared valid; here are the results:

Table 5. Results of *Cross Loadings*

Indicators	**Latent variable**			**Description**
	C.S.A. (X1)	D.S. (X2)	KBDB (Y)	
CSA14 (X1)	0,612	0,172	0,114	Valid
CSA15 (X1)	0,839	-0,011	0,160	Valid
CSA17 (X1)	0,883	0,218	0,253	Valid
CSA18 (X1)	0,812	0,227	0,173	Valid
DS1.4 (X2)	0,170	0,708	0,362	Valid
DS1.7 (X2)	0,073	0,635	0,236	Valid
DS1.8 (X2)	0,109	0,753	0,377	Valid
DS1.9 (X2)	0,114	0,812	0,273	Valid
DS1.11 (X2)	0,161	0,758	0,367	Valid

DS1.12 (X2)	0,234	0,765	0,303	Valid
DS2.1 (X2)	0,066	0,793	0,338	Valid
DS2.2 (X2)	0,068	0,635	0,178	Valid
DS2.3 (X2)	0,066	0,797	0,227	Valid
DS2.4 (X2)	0,083	0,885	0,320	Valid
DS3.1 (X2)	0,161	0,725	0,303	Valid
DS4.2 (X2)	0,246	0,622	0,404	Valid
DS4.3 (X2)	0,259	0,715	0,322	Valid
KBDB1.1 (Y)	0,147	0,229	0,668	Valid
KBDB1.3 (Y)	0,161	0,432	0,738	Valid
KBDB1.4 (Y)	0,155	0,401	0,778	Valid
KBDB1.5 (Y)	0,193	0,349	0,752	Valid
KBDB2.1 (Y)	0,065	0,238	0,748	Valid
KBDB2.2 (Y)	0,046	0,401	0,720	Valid
KBDB2.3 (Y)	0,168	0,225	0,756	Valid
KBDB2.4 (Y)	0,145	0,243	0,632	Valid
KBDB2.5 (Y)	0,241	0,286	0,879	Valid
KBDB3.1 (Y)	0,175	0,347	0,720	Valid
KBDB3.2 (Y)	0,371	0,181	0,663	Valid
KBDB3.3 (Y)	0,218	0,324	0,773	Valid

Source: processed data, 2020

b. Reliability test result

After the validity test stage, all latent variables are declared valid, and the next step is the reliability test. The latent variable is declared reliable if the values are composite reliability and *Cronbach alpha* above 0.7 (Ghozali 2014). The importance of composite reliability and *Cronbach alpha* in this study are above 0.7 so that the latent variables are reliable.

Table 6. Reliability Test Result

Variable	**Composite Reliability**	**Cronbach's Alpha**	**Description**
Cybersecurity Awareness (X1)	0,870	0,805	Reliable
Digital Skills (X2)	0,940	0,931	Reliable
Change Readiness in Digital Banking (Y)	0,934	0,923	Reliable

Source: Processed data, 2020

4.1.2 Evaluation of Measurement Model (*Outer Model*)

Evaluation of the measurement model in this study consists of the coefficient of determination (*R-Square*), the path coefficient test, and the t-statistical test (*bootstrapping*).

a. Determination of Coefficient Test (*R-Square* (R^2))

Table 7. Results of *R-Square* (R^2)

Variable	*R-Square* (R^2) value
Cybersecurity Awareness (X1)	
Digital Skills (X2)	
Change Readiness in digital banking (Y)	0,211

Source: processed data, 2020

Coefficient of Determination (*R-Square* (R^2)) shows how much influence exogenous latent variables have on endogenous latent variables. The table above test results shows R Square's value (R2) of this study is 0,211. This information means that the effect of the exogenous latent variable *cybersecurity awareness* (X1) and the exogenous latent variable *digital skills* (X2) on the endogenous latent variable readiness to change in *digital banking* (Y) is 21.1%, and other latent variables outside the model influence the remaining 78.9%. This research. According to Chin (1998), as cited in Ghozali (2014), the results of *R Square* (R^2) between 0,19-0,33 indicates that the model is moderate. *This study's R Square (R2) is 0,211, which is in between, so the structural quality of the research model* is average.

b. Path Coefficient Test

Table 8.Path Coefficient Test Result

Variable	Path coefficient test value	Description
Cybersecurity Awareness (X1)	0,154	Positive relationship
Digital Skills (X2)	0,404	Positive relationship

Source: processed data, 2020

Results of path coefficient values for exogenous latent variable *cybersecurity awareness* (X1) The endogenous latent variable Readiness for Change in *digital banking* (Y) shows a positive value of 0.154, meaning that the relationship between the exogenous latent inconsistent *cybersecurity awareness* (X1) and the endogenous latent variable readiness to change in *digital banking* (Y) is positive. While the path coefficient value of the exogenous latent variable digital skills (X2) on the endogenous latent variable readiness to change in digital banking (Y) shows a positive value of 0.404, meaning that the direction of the relationship between the exogenous

latent variable digital skills (X2) to the endogenous latent variable readiness to change in digital banking (Y) is also positive.

c. The statistical t-test (*Bootstrapping*)

b

Variable	T-test	P-Value	Description
Cybersecurity Awareness (X1)	1,190	0,117	Not significant
Digital Skills (X2)	4,127	0,000	Significant

Source: processed data, 2020

The T-test (Bootstrapping) is a significant test to test the hypothesis in this study. The t-table value in this study, with a confidence degree of 95% and degrees of freedom df = 101-3 = 98 for the one-way test, obtained a t-table value of 1.661. The test result is significant if the t-statistical value is greater than the t-table value and the p-value ‹0.05. Here are the results of the hypothesis:

- Hypothesis Testing of Exogenous latent variable of cybersecurity awareness (X1) towards endogenous latent variable of readiness to change in digital banking (Y)
- Based on the test results in the T-Statistics (Bootstrapping) table, the t-statistic value of the exogenous latent variable cybersecurity awareness (X1) is 1.190, so the t-statistic ‹t-table (1.190 ‹1.661). The p-value of the exogenous latent variable cybersecurity awareness (X1) is 0.117 so that the p-value is› 0.05 (0.117› 0.05). This result means that the exogenous latent variable cybersecurity awareness (X1) does not significantly affect the endogenous latent variable readiness to change in digital banking (Y). The path coefficient value shows a positive value of 0.154, meaning that the relationship between the exogenous latent variable cybersecurity awareness (X1) and the endogenous latent variable readiness to change in digital banking (Y) is positive. From the above analysis, it can be concluded that the first hypothesis is not accepted because although the exogenous latent variable cybersecurity awareness (X1) has a positive effect on the endogenous latent variable readiness to change in digital banking (Y), the t-statistic and p-value are not significant.
- Hypothesis Testing of Exogenous latent variable of digital skills (X2) on the endogenous latent variable of readiness to change in digital banking (Y).

Based on the test results in the T-Statistics (Bootstrapping) table, the t-statistic value of the exogenous digital skills (X2) latent variable is 4.127, so that the t-statistic› t-table (4.127› 1.661). The p-value of the exogenous digital skills (X2) latent variable is 0,000, so the p-value is ‹0.05 (0,000 ‹0.05). This finding means that the exogenous latent variable digital skills (X2) significantly affect the endogenous latent variable readiness to change in digital banking (Y). The path coefficient value shows a positive value of 0.404, meaning that the relationship between the exogenous latent variable digital skills (X2) and the endogenous latent variable readiness to change in digital banking (Y) is positive. From the analysis above, it can be concluded that the second hypothesis is accepted because the exogenous latent variable digital skills (X2) has a positive and significant effect on the endogenous latent variable readiness to change in digital banking (Y).

4.2 Discussion

The first hypothesis is not accepted (rejected) as the exogenous latent variable cybersecurity awareness does not affect change Readiness in Digital Banking. Although it does not have a significant effect, the correlation is positive, and the mean value of respondents' answers to the exogenous latent variable cybersecurity awareness is relatively high, namely 4.101. The respondents 'cybersecurity awareness's mean value shows that the respondents' cybersecurity awareness level is in a suitable category. Respondents were fresh college graduates born as generation Y (millennial) and Z. According to Bencsik and Machova (2016), the characteristics of the use of generation Y information technology cannot be separated from the use of information technology every day. Generation Z is quite intuitive or does not need to think for a long time automatically in its use (Putra 2016). High education and a technology responsive generation encouraged these respondents to be aware of cybercrime dangers on the internet. Security in banking information technology systems was hacked during the Covid-19 pandemic. One of the reasons is that the cybersecurity awareness of banking employees was less so that they were less alert when receiving online messages from unknown parties on bank computers (CNN Indonesia 2020). Cybersecurity awareness must be built in the banking culture. It must start when employees are recruited because employees are part of banking stakeholders, so it is essential if employees have security awareness (Babu 2018). If bank employees are accepted from the start, they already have cybersecurity awareness, and it will make it easier for the company if there is cybersecurity awareness training. Cybersecurity awareness competence is significant for banking employees, including sharia banking, because in the future, the banking business model will continue to change following technological developments, and this is accompanied by the increasing vulnerability of banking cybersecurity so that having human resources who are responsive to cybersecurity awareness is very important.

The second hypothesis is accepted as the exogenous latent variable. Digital Skills has a positive and significant effect on Change Readiness in Digital Banking. In the sharia banking roadmap prepared by the O.J.K. for 2015-2019 and the sharia banking road map made by KNEKS for 2020-2024, the same problems have become issues for Islamic banking in Indonesia, namely the lack of quality and quantity of human resources and technology in Islamic banking. in Indonesia compared to conventional banks which are much better (Departemen Perbankan Syariah O.J.K., 2015; Komite Nasional Keuangan Syariah, 2018). Considering that the age of Islamic banking in Indonesia is still younger than conventional banks, conventional banks are more stable in capital, and technology investment is an excellent value in banking. Islamic banking is yet to improve technology to catch up with the

advancement of conventional banks. The emergence of the Islamic banking department at universities in Indonesia is also an answer to the need for Islamic banking human resources that understand banking operations and Islamic economics. Human resources who have the competence of digital skills are an investment in the banking business that continues to transform into a digital business model (Gasser et al., 2017). Graduates who are competent and skillful in using information technology can drive cost efficiency in technology training.

Additionally, technology will have an impact on future banking jobs. Based on Accenture Research (2018), 97% of cashier (teller) jobs and 98% of loan officer jobs are likely to be automated by technology. Machines will mostly replace jobs in the banking sector, so technology-related skills are needed to remain competitive in a banking career. This finding is in line with the formulation of 21-st Century Skills that was created by the World Economic Forum (2016) that one of the skills needed in the 21st century is information and communication technology literacy, which is part of the information skills in the digital skills variable (van Dijk and van Deursen 2014).

5. Conclusion

This research shows that cybersecurity awareness has no effect on Change Readiness in Digital Banking and Digital Skills have a positive and significant impact on Change Readiness in Digital Banking. Prospective Islamic Banking human resources must have good quality Digital Skills because of the massive changes in the banking business model technologically. Although cybersecurity awareness does not have a significant effect, it positively correlates with Change Readiness in Digital Banking. Employees aware of cybercrime will minimize the risk to the company's technology security, especially the banking business, which must apply the principle of prudence because it is related to the management of very large third-party funds belonging to the public.

6. Recommendation

In terms of regulations, a curriculum that prioritizes the mastery of technology from beginner to intermediate levels must be implemented in study programs or departments outside the universities' Information Technology Technology Technology. In the problem of the lack of human resources quality for Islamic Banking in Indonesia, the road map for Islamic banking created by KNEKS for 2020-2024 also provides solutions for S.D.I. opportunities for university graduates majoring in Islamic Economics and related ones (Islamic Banking, Sharia Accounting, Sharia Business Management) which began to emerge a lot in Indonesia. This finding should be utilized by the managers of higher education institutions with Sharia Economics study programs and allied science to improve their graduates' technological

capabilities so that they are competitive and become a workforce ready to be accepted in the banking fintech business.

Academically, this research has many limitations. In further research, the theoretical framework that has been formed in this study can be added or modified with other exogenous and endogenous variables. The research sample can be tested on graduates other than Islamic Banking, such as Islamic Economics or majors related to conventional economics and outside economics, to increase data variation and further evaluation. Analysis tools can be developed through CB-SEM with a larger number of samples to compare the test results with the PLS-SEM-based analysis method.

References

Accenture Research. 2018. "Future Workforce Banking Survey | Realizing the Full Value of A.I."

Achilles A. Armenakis, Stanley G. Harris, and Kevin W. Mossholder. 1993. "Armenakis, Harris & Mossholder (1993) Creating Readiness for Organizational Change." *Human Relations* 46(6): 681–703.

Babu, Burra Butchi. 2018. "CYBERSECURITY IN BANKS." 89(01).

Bouckenooghe, Dave, Geert Devos, and Herman Van Den Broeck. 2009. 143 Journal of Psychology: Interdisciplinary and Applied *Organizational Change Questionnaire-Climate of Change, Processes, and Readiness: Development of a New Instrument*.

CNN Indonesia. 2020. "No Title." https://www.cnnindonesia.com/teknologi/20200723104339-185-528047/bank-dan-ukm-indonesia-jadi-sasaran-hacker-kala-pandemi (August 15, 2020).

Cooper, D.R., and P.S. Schindler. 2014. *Business Research Methods*. 12th ed. New York: McGraw-Hill Book.

Departemen Perbankan Syariah. 2015. "Roadmap-Pbs_2015-2019.Pdf." : 53. https://www.ojk.go.id/id/kanal/syariah/berita-dan-kegiatan/publikasi/Documents/roadmap-pbs_2015-2019.pdf.

van Deursen, A. J.A.M., and J. A.G.M. van Dijk. 2009. "Improving Digital Skills for the Use of Online Public Information and Services." *Government Information Quarterly* 26(2): 333–40. http://dx.doi.org/10.1016/j.giq.2008.11.002.

van Dijk, Jan A. G. M., and Alexander J. A. M. van Deursen. 2014. "Digital Skills." *Digital Skills* (November 2018).

Gasser, Urs et al. 2017. "Digital Banking 2025." (April). http://www.dv.co.th/blog-th/digital-banking-trend/.

Ghozali, Imam. 2014. *Structural Equation Modeling, Metode Alternatif Dengan Partial Least Squares (P.L.S.)*. 4th ed. Semarang: Badan Penerbit UNDIP.

Ghozali, Imam, and Hengky Latan. 2015. *Partial Least Squares : Konsep, Teknik, Dan Aplikasi Menggunakan Program SmartPLS 3.0 Untuk Penelitian Empiris*. Semarang: Badan Penerbit UNDIP.

Hair, Joseph F. Jr. et al. 2006. *Multivariate Data Analysis*. 6th ed. Upper Saddle River, New Jersey: Pearson Education, Inc.

Hair, Joseph F., Jeffrey J. Risher, Marko Sarstedt, and Christian M. Ringle. 2019. "When to Use and How to Report the Results of PLS-SEM." *European Business Review* 31(1): 2–24.

Holt, Daniel T., Achilles A. Armenakis, Hubert S. Feild, and Stanley G. Harris. 2007. "Readiness for Organizational Change: The Systematic Development of a Scale." *Journal of Applied Behavioral Science* 43(2): 232–55.

Hootsuite and We Are Social. 2020. "Digital 2020 : Indonesia." Hootsuite, We Are Social.

International Telecommunication Union (I.T.U.). 2018. *Digital Skills Toolkit*.

Ito, Joichi, Neha Narula, and Robleh Ali. 2017. "The Blockchain Will Do to the Financial System What the Internet Did to Media." *Harvard Business Review*. https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media.

Jones, jimmieson & Griffiths. 2005. "The Impact of Organizational Culture and Reshaping." *Journal of Management Studies* 42(2): 361–86.

Kementerian Komunikasi dan Informatika RI. 2020. "Terjadi Pergeseran Penggunaan Internet Selama Masa Pandemi." https://kominfo.go.id/content/detail/26060/terjadi-pergeseran-penggunaan-internet-selama-masa-pandemi/0/berita_satker.

Komite Nasional Keuangan Syariah. 2018. "Masterplan Ekonomi Syariah Indonesia 2019-2024." *Kementerian Perencanaan Pembangunan Nasional/ Badan Perencanaan Pembangunan*

Nasional: 1–443.

Kompas.com. 2020. "BSSN Catat Adanya 88,4 Juta Serangan Siber Selama Pandemi Corona." https://www.kompas.com/tren/read/2020/04/23/165400665/bssn-catat-adanya-88-4-juta-serangan-siber-selama-pandemi-corona?page=all.

Mapoka, Trust Tshepo, Keneilwe Zuva, and Tranos Zuva. 2019. "Hack the Bank and Best Practices for Secure Bank." *International Journal of Computer Science, Communication & Information Technology (CSCIT)* 7: 17–21.

Muhirwe, Jackson, and Nathan White. 2016. "Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users." *Issues in Information Systems* 17(Ii): 183–92.

NUI Galway. 2020. "I.T. and Digital Skills." http://www.nuigalway.ie/academic-skills/itskills/.

Osada, Hiroyasu. 1997. "Evaluation Method for Cyber Awareness Course Master." *October*: 21–23.

Otoritas Jasa Keuangan. 2016. "Panduan Penyelenggaraan Digital Branch Oleh Bank Umum." : 9.

Peker, Yesem Kurt, Lydia Ray, Stephanie Da Silva, and Nathaniel Gibson. 2016. "Raising Cybersecurity Awareness among College Students." *Journal of The Colloquium for Information System Security Education (CISSE)* (September): 1–17.

Putra, Yanuar Surya. 2016. "THEORITICAL REVIEW : TEORI PERBEDAAN GENERASI." *Among Makarti* Vol.9 No.1(1952): 123–34.

Ryerson. 2011. "Η Διοίκηση Αλλαγών (Change Management) Στο Δημόσιο Τομέα." *Εσδδ-Τμημα Γενικησ ΔΙοικησησ*. https://www.ryerson.ca/content/dam/hr/manager-resources/docs/change-management-leadership-guide.pdf.

Satria, Dias. 2018. "Inclusively Creative : Peran Bank Indonesia Dalam Perkembangan Ekonomi Inclusively Creative : Peran Bank Indonesia Dalam Pengembangan Ekonomi Digital Dan Teknologi Finansial." (September): 1–23.

Sekaran, Uma. 2011. *Research Methods for Business (Metode Penelitian Untuk Bisnis)*. Jakarta: Salemba Empat.

Shaw, R. S., Charlie C. Chen, Albert L. Harris, and Hui Jou Huang. 2009. "The Impact of Information Richness on Information Security Awareness Training Effectiveness." *Computers and Education* 52(1): 92–100. http://dx.doi.org/10.1016/j.compedu.2008.06.011.

Teer, Faye P., S. E. Kruck, and Gregory P. Kruck. 2007. "Empirical Study of Students' Computer Security Practices/Perceptions." *Journal of Computer Information Systems* 47(3): 105–10.

Vayansky, Ike, and Sathish Kumar. 2018. "Phishing – Challenges and Solutions." *Computer Fraud and Security* 2018(1): 15–20.

Wang, Yu, Bin Qi, Hong Xia Zou, and Ji Xing Li. 2019. "Framework of Raising Cyber Security Awareness." *International Conference on Communication Technology Proceedings, ICCT* 2019-Octob: 865–69.

Wirjoatmodjo. Kartika. 2018. Majalah Probank No.133. Edisi April-Juni 2018.

World Economic Forum. 2016. "What Are the 21st-Century Skills Every Student Needs?" https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students.