Imagine if security measures are difficult to implement, offer little evident benefit, or are ineffective at preventing people from taking advantage of situations for their gain. In that circumstance, users are likely to disregard the controls.

Besides, the study by Conolly et al. [24] identifies six factors influencing employee behavior regarding information security in an organization. The factors are values, norms, practices, organizational characteristics, individual characteristics, and individual values. The study is based on a framework that combines the taxonomy of organizational culture [25], Sarhan organizational culture model[26], Hofstede's original taxonomy of national culture [27], and Schwartz's Theory of Motivational Types of Values [28], as presented in Table II.

TABLE II
CONOLLY'S SIX INFLUENTIAL FACTORS

Factors	Descriptions
1. Values	Organizational values and Information Security Values
2. Norms	Norms typically result from values but are easier to see.
3. Practices	The level of implementation of particular values within the organization.
4. Organizational characteristics	Such as the sector and size of the organization.
5. Individual characteristics	Such as nationality and experience.
6. Individual values	Such as achievement, benevolence, conformity, and self-direction.

Another study by Funnel et al. [29] found that a combination of guidance and effective enforcement allows users to understand and accept security procedures but still cannot handle the problems of those who try to resist or remain unaware. Manik Rakhra, and Davneet Kaur [30] found that web security education and awareness of cybercrime among users play an essential role, requiring serious research in studying methods and techniques to teach users. One issue that needs attention is the users' level of understanding and awareness. A study by Farhad Foroughi and Peter Luksch [31] suggests the necessary observation steps get a user security behavior profile. These observations can then be analyzed utilizing data mining and machine learning methods.

C. Method

This research was conducted to ascertain the degree of user security behavior of employees in the service industry. The study was performed in the province of West Sumatra, Indonesia. This study considers three dimensions (knowledge, attitude, and behavior) with seven factors influencing user security behaviors. These factors are shown in Table III.

This study was carried out using a questionnaire survey. Respondents were randomly selected from four service sectors: government services, education services, banking services, and other private sector services. The questionnaire was distributed through email; respondents were also asked to return their answers through email. The questionnaire was distributed through email; respondents were also asked to return their answers through email.

TABLE III
FACTORS TO CONSIDERED IN THIS STUDY

No	Factors	Description
1	Values of the organization	Availability of security procedures and staff are told about the security procedure.
2	The behavior of the peers	Enforcement of security procedure
3	Ability to make decision	Staff are given authority to make decision Staff are given proper training
4	Availability of tool support	Security tools such as antivirus and firewall
5	Personal values and standard	Staff must possess good values and main a high standard of practice
6	Employee-employer relationship	Good employee and employer relationship
7	The Effort needed to comply	Security procedures must be easy to use

This study sets the total population of respondents as 1600 (N) people following the publication of West Sumatra Province in 2019. The Slovin formula is employed to select the number of samples as in Equation 1 where N is the total population and e is the tolerated margin of error [32]. The number of samples must be met and represented by n. This study uses a margin of error of 5% (e). The finding explains that the number of samples is 320 (n) respondents, as shown in Table IV.

$$n = \frac{N}{1+N(e^2)} \quad (1)$$

n = Sample size;
N = Population size;
e = Error tolerance

The number of samples can be distributed following some sectors (Table VII). The first sector is local government, which contributes about 24% of the total population. The second sector is private, which contributes about 21%. Meanwhile, the third and fourth sectors are education and banking, which contribute about 38% and 17%, respectively.

TABLE IV
DESCRIPTIVE STATISTICS

Factors	Code	*n*	Min	Max	Mean	Std. Deviation
EAT	EAT1	320	1	4	3.27	.702
	EAT2	320	1	4	3.58	.708
	EAT3	320	1	4	3.06	.667
	EAT4	320	1	4	3.59	.601
ES	ES1	320	1	4	3.33	.682
	ES2	320	1	4	3.23	.604
	ES3	320	1	4	2.98	.703
	ES4	320	1	4	3.30	.601
	ES5	320	1	4	3.30	.574
	ES6	320	1	4	3.17	.617
OD	OD1	320	1	4	3.15	.683
	OD2	320	1	4	3.13	.599
	OD3	320	1	4	3.32	.628
	OD4	320	1	4	3.15	.683
TS	TS1	320	1	4	3.23	.629
	TS2	320	1	4	3.19	.647
	TS3	320	1	4	3.45	.590
	TS4	320	1	4	3.20	.648

Factors	Code	*n*	Min	Max	Mean	Std. Deviation
PS	PS1	320	1	4	3.18	.564
	PS2	320	1	4	3.36	.542
	PS3	320	1	4	3.18	.564
	PS4	320	1	4	3.36	.542
PC	PC1	320	1	4	3.35	.552
	PC2	320	1	4	3.30	.534
	PC3	320	1	4	3.09	.649
	PC4	320	1	4	3.35	.552
TDC	TDC1	320	1	4	3.33	.528
	TDC2	320	1	4	2.98	.710
	TDC3	320	1	4	3.33	.528
	TDC4	320	1	4	2.98	.710

The questionnaires were distributed randomly to 350 respondents, but only 320 replies were received. These 320 respondents consisted of 78 respondents (24%) from the government sector, 66 respondents from the private sector (21%), 123 respondents from the education sector (38%), and 53 respondents from the banking sector (17%). There are two sections to the questionnaire; (A) Demographics of the respondents and (B) Factors influencing employees' security behaviors. The 30 questions in Section B were further divided into seven parts representing seven factors influencing user security behaviors. The distribution of the questions is shown in Table V.

TABLE V
SECTION B OF THE QUESTIONNAIRE

Factors	Variables	No. of Questions
1. Values of the organization	Employees are told (EAT)	4
2. The behavior of the peers	Employee See (ES)	6
3. Ability to make decision	Own Decision (OD)	4
4. Availability of tool support	Tools Support (TS)	4
5. Individual values and standard	Personal Standard (PS)	4
6. Employee-employer relationship	Psychological Contract (PC)	4
7. The Effort needed to comply	The Difficulty in Complying (TDC)	4

The questions are written sequentially, with a clear statement for each one using a Likert scale where 1 indicates 'strongly disagree,' and 4 indicates 'strongly agreement'. The analysis was performed by tabulating the respondents' responses. The score for each item is the percentage of those selecting (3) and (4). The score is divided into good (score ≥ 90%), enough (Score between 80% to 90%), and poor (Score less than 80%).

III. Results and Discussion

A. The Demographic

Demographic questions consist of gender, age, field of work, number of years of work experience, and domain. The value of a degree of error is checked to find out the amount of data that is error or empty. The results of a degree of error are shown in Table VI with the total amount of data being 320 and the degree of error being zero, which means there is no error.

TABLE VI
CASE PROCESSING SUMMARY

	Valid		Cases Missing		Total	
	n	Percent	n	Percent	n	Percent
Gender	320	100%	0	0.0%	320	100%
Age	320	100%	0	0.0%	320	100%
Field of work	320	100%	0	0.0%	320	100%
Number of years of work experience	320	100%	0	0.0%	320	100%
Domain	320	100%	0	0.0%	320	100%

The description of the data shows that the average age of the respondents is 35 with the youngest and oldest ages being 17 and 63. Then the gender sample of the respondents is 225 males and 95 females . The number of men is more than female, because male are more dominant at the job level marked by 17% Senior Manager, 27% Operational and 26% Transactional. In terms of working experience of the respondents, 37.5% are less than five years, 30.6% are between 6 to 10 years, 14.4% are between 11 to 15 years, 9.7% are between 16 to 20 years, and 7.8% are working for more than 20 years. Regarding employment, 24% work as government employees, 21% in the private sector, 38% in the educational sector, and 17% in banks. The respondents' demographics are as follows in Table VII.

TABLE VII
RESPONDENTS' DEMOGRAPHY

Respondents' Demographic	Frequency	Percentage
Gender		
Male	225	70.3%
Female	95	29.7%
Age		
Less 25 years	45	14.1%
25 - 30 years	68	21.3%
31 - 35 years	71	22.2%
36 - 40 years	57	17.8%
More 40 years	79	24.7%
The field of work		
Senior Manager	66	20.6%
Operational	133	41.6%
Transactional	121	37.8%
Working experience		
Less 5 years	120	37.5%
6 - 10 years	98	30.6%
11 - 15 years	46	14.4%
16 - 20 years	31	9.7%
More 20 years	25	7.8%
Domain		
Government	78	24%
Private sector	66	21%
Education	123	38%
Banking	53	17%

B. Scores For Factors That Influencing Employees' Security Behavior

Part B of the questionnaire is a query regarding seven factors influencing employees' security performance, as shown in Table V.

1) Values of the Organization: There are four questions in the questionnaire concerning the factor of the value of the organization:

- EAT1: The organization has a clear security procedure.
- EAT2: Importance of the security procedure
- EAT3: Importance of following the security procedure.
- EAT4: Need to ensure that the procedure is understood.

From the distribution of responses given in Table VIII, it seems that most organizations have clear security rules and procedures, and most employees feel that they do not have any problem understanding and following their organizations' security rules and procedures. However, only item EAT3 needs to be given some attention. The employees understand the importance of the security procedure, but they have a problem following the procedure.

TABLE VIII
RESULTS OF FACTOR VALUES OF THE ORGANIZATION

ITEM	Responses				Score
	1	2	3	4	
EAT1	11 (3.44%)	14 (4.38%)	172 (53.75%)	123 (38.44%)	92.19% (Good)
EAT2	12 (3.75%)	5 (1.56%)	89 (27.81%)	214 (66.88%)	94.69% (Good)
EAT3	3 (0.94%)	53 (16.56%)	186 (58.13%)	78 (24.38%)	82.50% (Enough)
EAT4	6 (1.88%)	1 (0.31%)	110 (34.38%)	203 (63.44%)	97.8% (Good)
Average					91.80%

2) Behavior of the peers: There are six questions related to the factor behavior of the peers. The questions are:

- ES1: Influence of seniors in the organization
- ES2: Influence of peers
- ES3: Support from peers
- ES4: Support from the organization
- ES5: Appreciation for good security behavior
- ES6: Penalty for poor security behavior

The distribution of responses is as in Table IX. The responses show that most employees do not have any problems with their seniors and peers. However, there seem to be issues concerning ES3 (Support from peers) and ES6 (Penalty for poor security behavior).

TABLE IX
RESULTS OF FACTOR BEHAVIOR OF THE PEERS

ITEM	Responses				Score
	1	2	3	4	
ES1	9 (2.81%)	12 (3.75%)	164 (51.25%)	135 (42.19%)	93.44% (Good)
ES2	5 (1.56%)	15 (4.69%)	202 (63.13%)	98 (30.63%)	93.8% (Good)
ES3	8 (2.50%)	59 (18.44%)	186 (58.13%)	67 (20/94%)	79.06% (Poor)
ES4	3 (0.94%)	15 (4.69%)	185 (57.81%)	117 (36.56%)	94.38% (Good)
ES5	2 (0.63%)	13 (4.06%)	192 (60.0%)	113 (35.31%)	95.3% (Good)
ES6	2 (0.63%)	32 (10.00%)	195 (60.94%)	91 (28.44%)	89.38% (Enough)
Average					90.89% (Good)

3) Ability to make decisions: Four questions are related to the factor's ability to decide. The questions are:

- OD1: Initiatives to solve a problem
- OD2: Knowledge of Security Problems
- OD3: Availability of supporting staff
- OD4: Looking for the best solution

The distribution of responses is as in Table X. From the responses. It seems that many employees are having some problems dealing with this factor. In particular, they have a problem finding initiatives to solve a problem. They feel that they lack proper computer security knowledge and are not confident in proposing the best solution for a problem.

TABLE X
FACTOR ABILITY TO MAKE DECISION

ITEM	Responses				Score
	1	2	3	4	
OD1	2 (0.63%)	48 (15.00%)	170 (53.13%)	100 (31.25%)	84.40% (Enough)
OD2	1 (0.31%)	36 (11.25%)	203 (63.44%)	80 (25%)	88.40% (Enough)
OD3	2 (0.63%)	22 (6.88%)	167 (52.19%)	129 (40.31%)	92.50% (Good)
OD4	2 (0.63%)	48 (15%)	170 (53.13%)	100 (31.25%)	84.40% (Enough)
Average					87.43% (Enough)

4) Availability of tool support: Four questions are related to the factor availability of tool support. The questions are:

- TS1: Use of security tools such as antivirus
- TS2: Use of firewall
- TS3: Using good passwords
- TS4: Encrypting confidential documents

The distribution of responses is as in Table XI. The result shows that most employees have no problem using support tools to do their work. However, they have a problem with encrypting confidential documents (TS4).

TABLE XI
RESULTS OF FACTOR AVAILABILITY OF TOOL SUPPORT

ITEM	Responses				Score
	1	2	3	4	
TS1	3 (0.94%)	26 (8.13%)	186 (58.13%)	105 (32.81%)	90.9% (Good)
TS2	6 (1.88%)	24 (7.50%)	193 (60.31%)	97 (3031%)	90.6% (Good)
TS3	2 (0.63%)	10 (3.13%)	150 (46.88%)	158 (49.38%)	96.3% (Good)
TS4	2 (0.63%)	35 (10.94%)	179 (55.94%)	104 (32.50%)	88.4% (Enough)
Average					91.6% (Good)

5) Individual values: There are four questions related to the factor of individual value.

- PS1: Ability to use a computer according to the

expected standard.

- PS2: Comfortable with the security procedure.
- PS3: Able to follow the given security procedure.
- PS4: Need for training

From the distribution of responses shown in Table XII, most employees seem to have good individual values and standards.

TABLE XII
RESULTS OF FACTOR INDIVIDUAL VALUES

ITEM	Score				S/SS
	1	2	3	4	
PS1	2 (0.63%)	21 (6.56%)	214 (66.88%)	83 (25.94%)	92.8% (Good)
PS2	2 (0.63%)	4 (1.25%)	191 (59.69%)	123 (38.44%)	98.1% (Good)
PS3	2 (0.63%)	21 (6.56%)	214 (66.88%)	83 (25.94%)	92.8% (Good)
PS4	2 (0.63%)	4 (1.25%)	191 (59.69%)	123 (38.44%)	98.1% (Good)
Average					95.5% (Good)

6) Employee-employer relationship: The distribution of responses in Table XIII shows that most employees feel an excellent employee-employer relationship in most organizations. However, there is a slight problem with PC3 regarding work promotion. This factor consists of four questions. The questions are:

- PC1: Carry out computer security procedures following company standards.
- PC2: Always do the work following the procedure until the next time.
- PC3: The work I do can increase productivity so that I get promoted
- PC4: I am used to working that is often done and trusted by the leadership

TABLE XIII
RESULTS OF FACTOR EMPLOYEE-EMPLOYER RELATIONSHIP

ITEM	Responses				Score
	1	2	3	4	
PC1	2 (0.63%)	6 (1.88%)	189 (59.06%)	123 (38.44%)	97.5% (Good)
PC2	3 (0.94%)	3 (0.94%)	210 (65.63%)	104 (32.50%)	98.1% (Good)
PC3	5 (1.56%)	39 (12.19%)	198 (61.88%)	78 (24.38%)	86.3% (Enough)
PC4	2 (0.63%)	6 (1.88%)	189 (59.06%)	123 (38.44)	97.5% (Good)
Average					94.8% (Good)

7) The Effort needed to comply. There are four questions related to the factor effort needed to comply. The questions are:

- TDC1: Have to face many problems to complete a given task.
- TDC2: Implementing security procedures.
- TDC3: Understanding security procedures.
- TDC4: Understanding instruction.

The distribution of responses is shown in Table XIV. The responses show that most employees struggle with the organization's security procedures.

TABLE XIV
RESULTS OF FACTOR EFFORT NEEDED TO COMPLY

ITEM	Responses				Score
	1	2	3	4	
TDC1	2 (0.63%)	3 (0.94%)	202 (63.13%)	113 (35.31%)	98.4% (Good)
TDC2	3 (0.94%)	75 (23.44%)	168 (52.50%)	74 (23.13%)	75.6% (Poor)
TDC3	2 (0.63%)	3 (0.94%)	202 (63.13%)	113 (35.31%)	98.4% (Good)
TDC4	3 (0.94%)	75 (23.44%)	168 (52.50%)	74 (23.13%)	75.6% (Poor)
Average					87.0% (Enough)

C. Summary

Figure 2 shows the summary results of those seven factors influencing user security behavior. All factors score above 80%. The lowest scores are the ability to make a decision (OD) and Effort needed to comply (TDC) factors with below 88%.

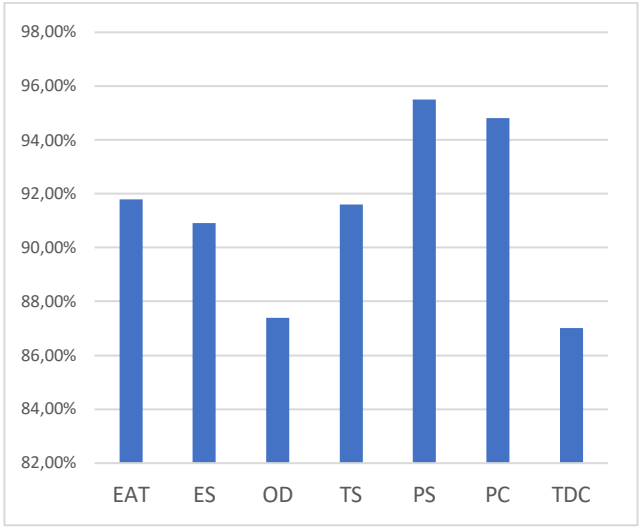

Fig. 2 Summary of the Result

D. Validity Test

The validity test is a test that aims to assess whether a set of measuring instruments correctly measures what should be measured. It consists of content and face validity. Content validity emphasizes the suitability of the contents of the measuring instrument with the topic measured by the measuring instrument concerned. Meanwhile, face validity refers to the extent to which the test looks correct and seems to measure the knowledge or ability that is considered to be measured, arguing that content validity is more appropriate than face validity. It is due to the notion that face validity is less stringent, and the only process involved is canceling the size and making the content valid based on the face size.

Therefore, this study chooses content validity to reveal the level of user behavior [33]. Checking content validity is used to ensure that the content of a measuring instrument is representative of the behavioral domain to be measured [34]. In contrast, face validity concerns whether the measuring instrument 'seems valid' to the people who want to use the instrument [35]

The normality test was carried out before the validity test using the Shapiro-Wilk test, which has a significant value of all items of 0.00, so it is smaller than 0.05, and it can be stated that the data is not normally distributed. The validity test in this study is done by checking content validity. Checking content validity is used to ensure that the content of a measuring instrument is representative of the behavioral domain to be measured. The validity test is employed using Pearson Product Moment Correlation. Pearson correlation or correlation value between the item is denoted by r. An item can be valid if the value r count ≥ r table with $\alpha = 0.05$, df (n-2)=318, resulting: 0.1097. The findings show that all factors are valid (Table XV).

TABLE XV
VALIDITY TEST

Factors	Code	*r count* n=320	Status
EAT	EAT1	0.371979	Valid
	EAT2	0.275374	Valid
	EAT3	0.240698	Valid
	EAT4	0.356448	Valid
ES	ES1	0.415137	Valid
	ES2	0.380189	Valid
	ES3	0.305621	Valid
	ES4	0.485149	Valid
	ES5	0.461203	Valid
	ES6	0.369895	Valid
OD	OD1	0.330687	Valid
	OD2	0.410942	Valid
	OD3	0.487002	Valid
	OD4	0.330687	Valid
TS	TS1	0.41196	Valid
	TS2	0.395058	Valid
	TS3	0.353897	Valid
	TS4	0.402502	Valid
PS	PS1	0.447248	Valid
	PS2	0.407328	Valid
	PS3	0.447248	Valid
	PS4	0.407328	Valid
PC	PC1	0.46254	Valid
	PC2	0.492598	Valid
	PC3	0.320012	Valid
	PC4	0.46254	Valid
TDC	TDC1	0.799	Valid
	TDC2	0.894523	Valid
	TDC3	0.799	Valid
	TDC4	0.894523	Valid

Note : r count ≥ r table means that the data are valid.

Table XIV shows the content validity test of user security behavior for 320 respondents. It reveals that all data are valid. The finding means that the data are normally distributed. Consequently, the employee-employer relationship can be estimated to address the study objective.

E. Reliability Test

The reliability of the test score is the consistency level between two measurement results on the same object[36]. One of the reliability measurements is Cronbach's Alpha value [37]. Cronbach's alpha reliability describes the dependability of a total (or average) of q measures, where the q measurements may reflect q raters, occasions, alternate forms, or questionnaire/test items. When Cronbach's Alpha score is 0.7 or more, it is said that the item provides a high enough level of reliability, but on the other hand, if the score is below 0.7, then the item is said to be less reliable. A reliability test was conducted from our survey is shown in Table XVI.

TABLE XVI
RELIABILITY TEST

Factor	Cronbach's Alpha Score
EAT	0.715
ES	0.844
OD	0.783
TS	0.751
PS	0.890
PC	0.820
TDC	0.866

Based on Table XVI, the reliability test of items regarding all factors obtained a Cronbach's Alpha score of higher than 0.7, so these items can provide a high level of reliability.

IV. CONCLUSION

This research aims to understand and find the level of user security behavior in the service industry. This study was conducted using a questionnaire survey method. This study considers seven factors that can influence user security behavior. These factors are the values of the organization, peers' behaviors, ability to make decisions, availability of tool support, individual values and standards, employee-employer relationship, and Effort needed to comply.

The findings indicate that the level of user security behavior is reasonably high. This implies that employees in the service industry in Indonesia are aware of the threats in cyberspace and the importance of the security procedure at work. However, eleven aspects need further investigation. These aspects are the importance of the security procedure (EAT2), the importance of following the security procedure (EAT3), Support from peers (ES3), Penalty for poor security behavior (ES6), Initiatives to solve a problem (OD1), Knowledge on Security Problems (OD2), Looking to the best solution (OD4), Encrypting confidential documents (TS4), productivity and promotion (PC3), Implementing security procedures (TDC2) and Understanding instruction (TDC4).

This study is vital to authorize service industry employees to figure out the urgencies to protect information security. In the future, we plan to study further some aspects of security behavior and possible solutions or actions to improve cyber user awareness.

ACKNOWLEDGMENT

The authors thank the Yayasan Universitas Putra Indonesia "YPTK" Padang and Universiti Kebangsaan Malaysia for supporting this research.

REFERENCES

[1] W. A. Al-khater, S. Member, S. A.- Ma, S. Member, K. Khan, and S. Member, "Comprehensive Review of Cybercrime Detection Techniques," *IEEE Access*, vol. XX, 2020, doi: 10.1109/ACCESS.2020.3011259.

[2] J. Brands and J. Van Doorn, "The measurement, intensity and determinants of fear of cybercrime: A systematic review," *Comput. Human Behav.*, vol. 127, p. 107082, 2022, doi: 10.1016/j.chb.2021.107082.

[3] T. B. G. Herath, P. Khanna, and M. Ahmed, "Cybersecurity Practices for Social Media Users: A Systematic Literature Review," *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 1–18, Jan. 2022, doi: 10.3390/jcp2010001.

[4] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions," *ACM Comput. Surv.*, vol. 54, no. 11s, pp. 1–37, Jan. 2022, doi: 10.1145/3514229.

[5] A. Chernikova *et al.*, "Cyber Network Resilience Against Self-Propagating Malware Attacks," in *European Symposium on Research in Computer Security*, Springer, 2022, pp. 531–550.

[6] S. Kamil, H. S. A. Siti Norul, A. Firdaus, and O. L. Usman, "The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges," in *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, Feb. 2022, pp. 1–7, doi: 10.1109/ICBATS54253.2022.9759000.

[7] Y. Hong and S. Furnell, "Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 19–28, 2022, doi: 10.1080/08874417.2019.1683781.

[8] H. Suryotrisongko and Y. Musashi, "Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective," *Proc. - 2019 IEEE 12th Conf. Serv. Comput. Appl. SOCA 2019*, pp. 162–167, 2019, doi: 10.1109/SOCA.2019.00031.

[9] L. Sanny, V. Angelina, and B. B. Christian, "Innovation of SME service industry in Indonesia in improving customer satisfaction," *J. Sci. Technol. Policy Manag.*, vol. 12, no. 2, pp. 351–370, 2021, doi: 10.1108/JSTPM-03-2020-0056.

[10] R. F. Ali, P. D. D. Dominic, S. Emad, A. Ali, and M. Rehman, "applied sciences Information Security Behavior and Information Security Policy Compliance : A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance," *Appl. Sci.*, 2021.

[11] I. Metin-Orta and D. Demirtepe-Saygılı, "Cyberloafing behaviors among university students: Their relationships with positive and negative affect," *Curr. Psychol.*, no. 0123456789, 2021, doi: 10.1007/s12144-021-02374-3.

[12] S. Toker and M. H. Baturay, "Factors affecting cyberloafing in computer laboratory teaching settings," *Int. J. Educ. Technol. High. Educ.*, vol. 18, no. 1, 2021, doi: 10.1186/s41239-021-00250-5.

[13] S. Asongu, C. Meniago, and R. Salahodjaev, "The role of value added across economic sectors in modulating the effects of FDI on TFP and economic growth dynamics," *Int. J. Emerg. Mark.*, 2022, doi: 10.1108/IJOEM-10-2018-0547.

[14] C. Chang, "Relational bonds , customer engagement , and service quality," *Serv. Ind. J.*, vol. 41, no. 321, pp. 330–354, 2021.

[15] A. da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, "Defining organisational information security culture—Perspectives from academia and industry," *Comput. Secur.*, vol. 92, p. 101713, 2020, doi: 10.1016/j.cose.2020.101713.

[16] E. Ukwandu *et al.*, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," *Inf.*, vol. 13, no. 3, pp. 1–22, 2022, doi: 10.3390/info13030146.

[17] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101640.

[18] G. Carmi and D. Bouhnik, "The Effect of Rational Based Beliefs and Awareness on Employee Compliance with Information Security Procedures: A Case Study of a Financial Corporation in Israel," *Interdiscip. J. Information, Knowledge, Manag.*, vol. 15, pp. 109–125, 2020, doi: 10.28945/4596.

[19] V. Hooper and C. Blunt, "Factors influencing the information security behaviour of IT employees," *Behav. Inf. Technol.*, vol. 39, no. 8, pp. 862–874, Aug. 2020, doi: 10.1080/0144929X.2019.1623322.

[20] Z. Ahmad, T. S. Ong, T. H. Liew, and M. Norhashim, "Security monitoring and information security assurance behaviour among employees," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 165–188, Jun. 2019, doi: 10.1108/ICS-10-2017-0073.

[21] M. Karjalainen, M. Siponen, and S. Sarker, "Toward a stage theory of the development of employees' information security behavior," *Comput. Secur.*, vol. 93, p. 101782, Jun. 2020, doi: 10.1016/j.cose.2020.101782.

[22] S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telemat. Informatics*, vol. 41, pp. 55–69, Aug. 2019, doi: 10.1016/j.tele.2019.03.003.

[23] J. Leach and J. Leach, "Improving user security behaviour," *Comput. Secur.*, vol. 22, no. 8, pp. 685–692, 2003.

[24] L. Connolly, M. Lang, J. Gathegi, and J. D. Tygar, "The effect of organizational culture on employee security behaviour: A qualitative study," *Proc. 10th Int. Symp. Hum. Asp. Inf. Secur. Assur. HAISA 2016*, no. March 2018, pp. 33–44, 2016.

[25] M. J. Alotaibi, S. Furnell, and N. Clarke, "A framework for reporting and dealing with end-user security policy compliance," *Inf. Comput. Secur.*, vol. 27, no. 1, pp. 2–25, Mar. 2019, doi: 10.1108/ICS-12-2017-0097.

[26] N. Sarhan, A. Harb, F. Shrafat, and M. Alhusban, "The effect of organizational culture on the organizational commitment: Evidence from hotel industry," *Manag. Sci. Lett.*, vol. 10, no. 1, pp. 183–196, 2020, doi: 10.5267/j.msl.2019.8.004.

[27] G. Hofstede, "Culture's Consequences:International Differences in Work-related Values," *Sage Publ. Thousand Oaks*, 1980.

[28] S. H. Schwartz, "Universal In The Content And Structure Of Values : Theoretical Advances And 20 Countries," vol. 25, 1992.

[29] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, "Enhancing security behaviour by supporting the user," *Comput. Secur.*, vol. 75, pp. 1–9, Jun. 2018, doi: 10.1016/j.cose.2018.01.016.

[30] M. Rakhra, "Behaviour In Developing An Effective Anti-Phishing Educational Framework," no. Icisc, pp. 832–836, 2018.

[31] F. Foroughi and P. Luksch, "A Multi-agent Model for Security Awareness Driven by Home User's Behaviours," in *Advances in Intelligent Systems and Computing*, vol. 880, Springer International Publishing, 2019, pp. 185–195.

[32] P. Uwayo, V. M. Nsanzumukiza, A. Maniragaba, A. P. Nsabimana, and V. Akimanizanye, "Contribution of Former Poachers for Wildlife Conservation in Rwanda Volcanoes National Park," *J. Geosci. Environ. Prot.*, vol. 08, no. 04, pp. 47–56, 2020, doi: 10.4236/gep.2020.84004.

[33] D. McGartland Rubio, "Content Validity," in *Encyclopedia of Social Measurement*, vol. 1, Elsevier, 2005, pp. 495–498.

[34] Livingston, S. A, "Test reliability—Basic concepts," (Research Memorandum No. RM-18-01). Princeton, NJ: Educational Testing Service, 2018.

[35] S. Giap, M. Ang, L. Anthony, and P. O. Brien, "Investigating the psychometric properties of the Carers ' Fall Concern instrument to measure carers ' concern for older people at risk of falling at home : A cross-sectional study," no. August 2019, pp. 1–10, 2020, doi: 10.1111/opn.12338.

[36] E. K. Titov and V. Y. Tsvetkov, "Accumulated reliability of information hardware and software systems," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 919, no. 2, p. 022055, Sep. 2020, doi: 10.1088/1757-899X/919/2/022055.

[37] E. A. O. Zijlmans, J. Tijmstra, L. A. van der Ark, and K. Sijtsma, "Item-Score Reliability as a Selection Tool in Test Construction," *Front. Psychol.*, vol. 9, no. JAN, Jan. 2019, doi: 10.3389/fpsyg.2018.02298.