How to Cite:
Abdelkader, S., & Boumediene, B. (2024). Analysis of cybersecurity factors for digital banking services in Algeria: Field study for local development bank client sample (BDL) in Ghardaia. *International Journal of Economic Perspectives*, *18*(11), 2396–2415. Retrieved from https://ijeponline.org/index.php/journal/article/view/725

Analysis of cybersecurity factors for digital banking services in Algeria: Field study for local development bank client sample (BDL) in Ghardaia

Souag Abdelkader
Laboratory of Quantitative and Qualitative Applications for the Economic, Social and Environmental Advancement of Algerian Institutions, University of Ghardaia, Algeria
Email: Souag.abdelkader@univ-ghardaia.dz

Boudaoud Boumediene
Research Center for Islamic Sciences and Civilization in Laghouat, Algeria
Email: b.boudaoud@crsic.dz

***Abstract*---**The study aims to know and analyse the cybersecurity factors of digital banking services in Algeria for the Local Development Bank (BDL) customer sample in the state of Ghardaia. In order to achieve these objectives, the questionnaire was distributed to a single form of (214). The "SEM" Structure Equation Modeling method was used by testing the confirmatory working form and testing the validity, honesty and stability of the study form using the "SPSS 26" statistical programme for social science, supplemented by "Amos 26". The study came up with the proposal of a cybersecurity form for Algeria's digital banking services consisting of the following dimensions: (Privacy Respect, Data Confidentiality, Technology Used, Availability & Sustainability, Traceability). Hence the researcher of Algeria's banking system proposes to adopt the proposed form of its five components as necessary elements in the production process of digital banking services, in order to ensure their safety and enjoyment of all quality characteristics. In addition, the client prefers to deal with the bank that provides reliable and secure electronic services.

***Keywords*---**Cybersecurity, Digital Banking Services, Bank Customers, Factor Analysis, Proposed Form.

Submitted: 27 September 2024, Revised: 09 October 2024, Accepted: 18 November 2024

1. Introduction

Security is the cornerstone of any society, so that the growth of any activity cannot be envisaged beyond its realization. Whether at the technical or legal level and security has been transformed with the emergence of the information society and cyberspace into one of the services sectors that is an added value and a mainstay of all different activities, as with e-government applications, e-health, e-education, e-commerce, etc.

Transforming societies into information societies is the transformation due to the integration of new technologies into each area of activity and into each type of infrastructure to increase individuals, organizations and countries' dependence on information systems and networks, a major source of risk that must be treated as a security risk.

Networked information technology systems are remotely accessible resources, hence potentially attacked or compromised cyberattacked targets, which can compromise the Organization's processing, production and storage capacity and even harm its decision-making processes.

Banking Organization of Algeria is not immune from the threats posed by the modern technological revolution, which has made it one of its priorities in protecting its structures while offering its digital services in a safe and reliable manner and in line with the desires of its customers, which prompts us to look for the most important components of cybersecurity in the Algerian banking environment. Based on this proposal, the following cognitive problems arise:

What are the most important components of cybersecurity in the banking environment of Local Development Bank BDL Ghardaia State?

The following sub-questions fall under this main problem:

1) Is Privacy Respect a dimension of cybersecurity for the Local Development Bank's banking environment (BDL) in Ghardaia?
2) Is Data Confidentiality a dimension of cybersecurity for the Local Development Bank's banking environment (BDL) in Ghardaia?
3) Is Technology Used a dimension of cybersecurity for the Local Development Bank's banking environment (BDL) in Ghardaia?
4) Is Availability & Sustainability a dimension of cybersecurity for the Local Development Bank's banking environment (BDL) in Ghardaia?
5) Is Traceability a dimension of cybersecurity for the Local Development Bank's banking environment (BDL) in Ghardaia?

1.1) Research hypotheses:

To answer the questions previously raised, we will use the following study hypotheses:

- Privacy Respect is a dimension of cybersecurity of the Local Development Bank's banking environment (BDL) in Ghardaia.
- Data Confidentiality is a dimension of cybersecurity of the Local Development Bank's banking environment (BDL) in Ghardaia.

- Technology Used is a dimension of cybersecurity of the Local Development Bank's banking environment (BDL) in Ghardaia.
- Availability & Sustainability is a dimension of cybersecurity of the Local Development Bank's banking environment (BDL) in Ghardaia.
- Traceability is a dimension of cybersecurity of the Local Development Bank's banking environment (BDL) in Ghardaia.

1.2) Research Objectives:

By answering questions about the study's problem, the study aims to:

- Enriching scientific knowledge in cybersecurity field.
- Learning about the Local Development Bank's reality (BDL) of cybersecurity field in Ghardaia State Algeria.
- Implementation of the proposed form of cybersecurity dimensions in Algeria's banking environment.
- Analyze the dimensions of cybersecurity and determine its availability in the Algerian banking environment.
- Discover the relationship between the dimensions of cybersecurity in the proposed form of the study.
- Provide decision makers in Algeria's banking system with the importance of cybersecurity through the adoption of its five dimensions.

1.3) The Importance of Research:

The topic is of great importance in view of the following:

- The importance of the banking sector at present, where banks are the primary drivers of development finance operations.
- The need to provide a cybersecurity component in digital transactions.
- Cybercrime in general has increased in all digital activities in Algerian society, especially in the financial sector.
- Absence of the adequate field studies to study the dimensions of cybersecurity and measure their availability in Algerian commercial banks.

1.4) The Study Form:

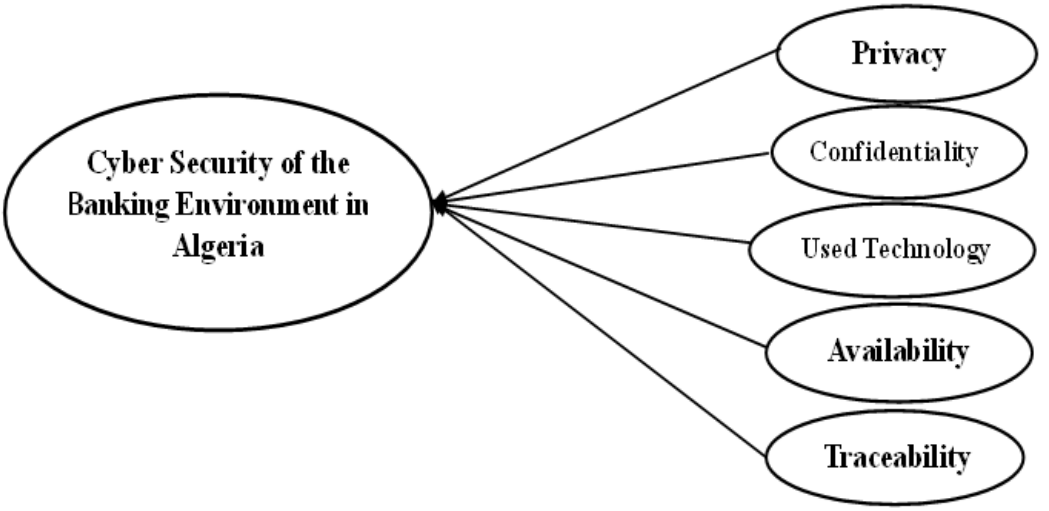

Figure No. (01): The Study Form Dimensions of Cybersecurity
Source: Prepared by researchers based on previous studies

2. Theoretical aspect:

2.1) Cybersecurity Concept:

It is a terminology that has been defined as a multiplicity of the definitions given to it, the term "Cyber" is a Greek-based term derived from the word "Kubernetes - Κυβερνήτεσ-", which means command or control. Source: "Cybernetics" means: "Communications science and automated control systems in both machines and living objects" (Lehto and Neittaanmaki, 2015, P 8).

The United States Department of Defense provided a definition of the term "cybersecurity", where it considered it: "all regulatory actions necessary to ensure the protection of information in all its forms (electronic and physical) from various crimes, attacks, sabotage, espionage and accidents" (Daniel Ventre, 2011, P 103).

The European Declaration considered cybersecurity as: "The ability of the information system to resist attempts at hacking or unexpected incidents targeting data" (Douwe Korff, 2015, P 1).

The Algerian legislator also defined cybersecurity as: "The whole range of tools, policies, concepts of security, security mechanisms, guidelines, risk management methods, business, good practices, composition, safeguards and technologies that can be used to protect electronic communications against any event that undermines the availability, integrity and confidentiality of processed, stored or transmitted data" (Official Gazette, Law No. 18-04, 2018). For the foregoing, through previous definitions we can conclude that:

- Cybersecurity is an activity or service that secures and protects ICT-related resources.

- Cybersecurity reduces material damage and financial losses resulting from risks or attacks in cyberspace.
- After the incident, cybersecurity restores the situation as soon as possible.
- The goal of cybersecurity is that the facility does not stop the production process whatever the situation.

2.2) Dimensions of cybersecurity:

We can define the dimensions of cybersecurity as the set of elements to be made available for data protection, so that each of these elements covers one aspect of the required protection, thus complementing these elements so as to provide protection and if any of them are lost, this will lead to a security imbalance, so that it must have five elements: (Mona Al-Ashqar Jabbour, 2019, p. 18)

2.2.1) Privacy Respect (PRIVACY):

It is difficult to establish an exhaustive and comprehensive definition of the right to privacy or the right to private life. The definition of this right is linked to prevailing traditions, cultures and religious values as well as the political system in each society. Privacy expresses customers' right not to publish or transmit their personal data relating to their dealings or private life such as activity, whereabouts, personal relationships, or even recording and wiretapping by electronic means. For example, privacy in banks is respected from asking for a private password when creating an account on the commercial banks' main website to various e-payment card transactions. There are also several technological solutions that are used to achieve personal data privacy.

The privacy policy should be to build and enhance customers' confidence in cyberspace. The level of this trust affects the quality and volume of data obtained. The client does not submit his data to any party. This is valued only for value or benefit. Any online store seeks to obtain accurate and credible data or information and this is achieved only through customer confidence. Attention to preserving the right to privacy is due to the beginning of the usage of ICT and the establishment of personal databases (Said Ziosh, 2023, p. 10).

2.2.2) Data Confidentiality (Confidentiality):

Also means preserving information and data from being accessed (read and understood) other than authorized persons or in other words unauthorized disclosure. When a confidential message is sent, it requires that only the sender and the addressee see it. But if anyone has access to it, he cannot understand its content. meaning must be incomprehensible. Confidentiality is also ensured by the level of protection required in each component of data and information processing. This level of protection must be available at all stages of processing to include stored data and information, data and information sent, as well as those that have reached its final destination.

There are also many ways to provide an element of secrecy. It ranges from manually withholding information and delivering it only to authorized persons to new or modern encryption methods based on complex mathematical algorithms

that are difficult to disassemble. Hence, we can say that the confidentiality element can be provided by encrypting data either fixed or transferred with the implementation of a strict access control policy. It also classifies information and trains workers on well-trained cybersecurity systems and policies.

2.2.3) Technology Used:

Means the service through which information and data are kept safe from any modification, deletion, addition, guidance or re-installation. This is very important to ensure confidence in information and that it is the original without increasing or decreasing. This information may be encrypted and confidential. But this information may be subject to change as long as it's electronic, Therefore, there is a need to find a way to detect this change, which is provided by the element of technology used through the accuracy and integrity of the processing systems from manipulation or unauthorized change. This also requires that different software, networking systems and devices operate in full harmony, also to preserve, process and transfer data and information to their intended destination without any modification or change, as well as to prevent manipulation. There must be a method of certifying that it has not been altered or modified during storage or transportation (Thaib Ben Ayad Al-Qahtani, 2015, p. 91).

2.2.4) Availability & Sustainability:

The availability of the information is intended to be accessible for use when requested by any person or specific and known entity and at any time authorized. We can say that the availability service is that service that protects the system to always be available. Hence, they are sometimes called sustainability and is specifically directed at any attack or imbalance that may result in the unavailability, interruption and disruption of services. For example, virus attacks and attacks that block, disable or block the service (Denial of Service-DoS). This challenge often requires physical and technical protection, such as technologies to provide backup information and power systems. The overall objective of the availability and sustainability element is to ensure that different networks, devices, systems, software and services are available at all times when needed by the user as well as to ensure the availability of systems, services and data. Therefore, appropriate sizes must be determined to protect the infrastructure, and provide operational management of resources, in the sense of keeping the data available to the user with access at any time without disruption due to a flaw in the database systems or means of communication.

Thus, the procedures for maintaining equipment, providing backups and upgrading operating systems to the latest versions for banks are preventive so that the bank does not fall into the problem of outages. Kits must also be prepared to overcome man-made disasters such as vandalism, arson or natural disasters such as earthquakes and floods (Osama Hussamuddin, 2017, p. 10).

2.2.5) Traceability:

It is the service through which it is ensured that no one who has performed a transaction or conduct connected with the data or its sites is denied (Merizeq

Adman, Imad Bukalashi, 2011, p. 4). The service of non-denial reveals this easily, in other words, providing the ability to demonstrate the interactive process through "The Traceability" tracking process.

To clarify further, if a message is sent between two parties, the technological effect proves the sender's transmission as well as the recipient's receipt, so that neither of them can deny it, and the importance of this proof increases as the message itself becomes more important, in addition to the actor's capability, traceability and auditability to determine liability. The Traceability service or a non-denial service also includes proof of the occurrence of electronic operations at certain dates and times by attaching a time and date imprint to the process itself (Time Stamping). If a particular electronic operation is carried out at a given date and time and then denies that it was performed at that time and date, this will be disclosed by reference to the original time and date print, called the system's auditability.

3. Digital Banking Services at Local Development Bank (BDL) in Ghardaia:

3.1) Digital Banking Concept:

Michael Amos Olushola defined it as: "It is the provision of products and banking services electronically and directly to customers wherever they are. May be Online Services, Virtual Services, Computer Services, Home Services, Remote Services, Telephone Banking Services, and many terms are used to describe them" (Amos Olushola Michael, 2020, P 79).

3.2) Types of Digital Banking Services:

There are several digital banking services offered by Local Development Bank (BDL) in Ghardaia to its customers, including:

- **ATM Service: Automatic Teller Machine**
  It is the most widely used electronic service. It is a programmed machine in which cash is kept and can identify its magnetic cards, provided by banks in most of its branches with the aim of reducing work pressure and avoiding administrative procedures and meeting customers' financial needs after working times and during the holidays.
- **Phone Banking Service: Phone Banking**
  This service grants the customer the right to dial the bank through a telephone connected to the bank's central computer, and enables the customer to request the operation or service he wants without the personal recourse of the bank.
- **SMS Service:**
  It is a new technology that allows the customer to follow all his or her banking transactions made on his or her personal account by receiving a text message from the bank on his or her mobile phone. The most important messages are: salary transfer, cash deposit, cash withdrawal, transfers between accounts... etc.
- **Point of Sale Service:**
  An automated payment device connected to an electronic network with banks is used in which money is transferred electronically from the customer's (buyer's) account to the merchant's account using the bank card, where the

customer uses it when paying for the services and goods he receives at shops, restaurants and other commercial facilities.

Internet Banking: Banking Online

This service allows customers through the Bank's website to deal with and inquire about their accounts from their personal devices in homes, shops or offices, through a special PIN for each of them. Customers can handle their own information and thus control their money, as well as enable them to browse, search and print any transaction.

- **Digital Transfers:**
  Transferring funds between two bank accounts or two financial portfolios by using the (GAB) device through different bank magnetic cards or by phone or mobile.
- **MoneyGram Service:**
  It is a service that allows the transfer of customers' funds in an easy and quick manner from any country abroad to Algeria in order to receive their funds through local development bank agencies (BDL) located across the entire national territory.

4. The Field Study:

4.1) The Study Community and Sample:

The study community consists of Local Development Bank (BDL) in Ghardaia customers using at least one e-service, where a simple random sample was selected, after the distribution of 220 questionnaires from which 214 processable identifications were retrieved, meaning that with a recovery rate: 97, 27%, which is very high.

4.2) Proposed Scale Form:

Drawing on Amos v22 outputs, the graphic format of the confirmatory working analysis illustrates the relationship between the dimensions of cybersecurity with the paragraphs or indicators expressed as illustrated in figure No. (02):

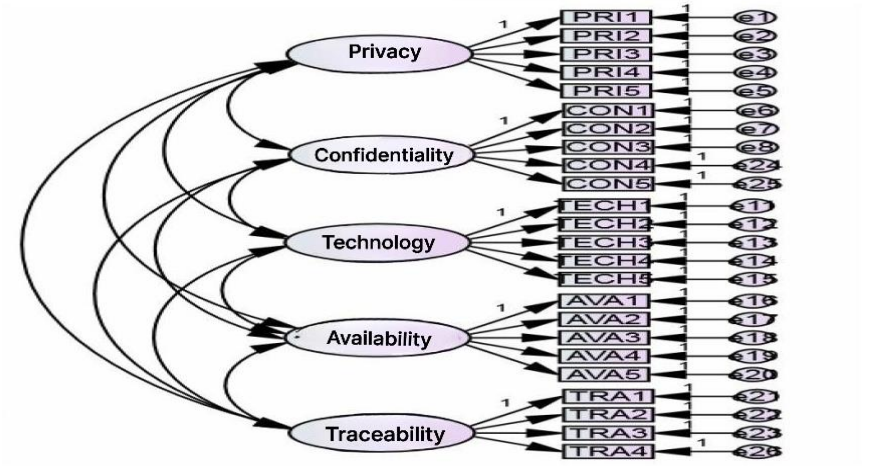

Figure No. (02): The Confirmatory factor analysis Form for Cybersecurity Dimensions
Source: Prepared by researchers based on Amos v26 outputs

4.3) Scale:

The survey used the quinquennial Card Scale, the study was given the following grades for the paragraphs used in the identification as follows:

Table No. (01): Grades of Questionnaire Paragraphs

Grade (1)	Grade (2)	Grade (3)	Grade (4)	Grade (5)
Strongly Disagree	Disagree	Impartial	Agree	Strongly Agree

Source: Prepared by researchers on the basis of The Card Scale

These averages are rated and graded according to the following standard:
Response range (1-5) was divided into three categories of equal length, based on the following arithmetic base:
Category Length = Range/Number of Categories.
Thus, the category's length is = 4/3 = 1.33 and the scale of analysis is as follows:

- Arithmetic Average is considered to be low if it ranges between: [1,00 - 2,33].
- Arithmetic Average is considered to be average if it ranges between: [2,34 - 3,66].
- Arithmetic Average is considered to be high if it ranges between [3,67-5,00].

4.4) Cronbach's Alpha Coefficient Test:

To ascertain the stability of the scale tool used in the study, Cronbach's alpha coefficient was calculated for the dimensions of the study. The results of the statistical analysis showed that the level of stability was high according to the accepted statistical standards, reaching 932, which exceeds 93%, making the standard very acceptable.

Table No. (02): Cronbach's Alpha Coefficient Totally Test for Paragraphs
Reliability Statistics

Cronbach's Alpha	The Number of Elements
,932	36

Source: Prepared by researchers based on SPSS v26 outputs

The Stability of the paragraphs was as follows:

Table No. (03): The detailed transactions of Cronbach's Alpha with the dimensions of the study

The Axis	Number of Paragraphs	Cronbach's Alpha Stabilization Coefficient
Dimensions of cybersecurity:	24 paragraphs distributed as follows:	
• Privacy Respect	05 paragraphs	0.823
• Data Confidentiality	05 paragraphs	0.713
• Technology Used	05 paragraphs	0.774
• Availability	05 paragraphs	0.727
• Traceability	04 paragraphs	0.726

Source: Prepared by researchers based on SPSS V26 outputs

5. The Confirmatory factor analysis of cybersecurity dimensions:

The Confirmatory factor analysis form, or stabilization form will be used to verify the veracity of the metrics used in the survey, test the confirmatory factor form showing whether the proposed factor structure of the scale matches the data, and provide the measured concept of good data conformity is one of the strongest pieces of evidence of constructive honesty, or concept sincerity.

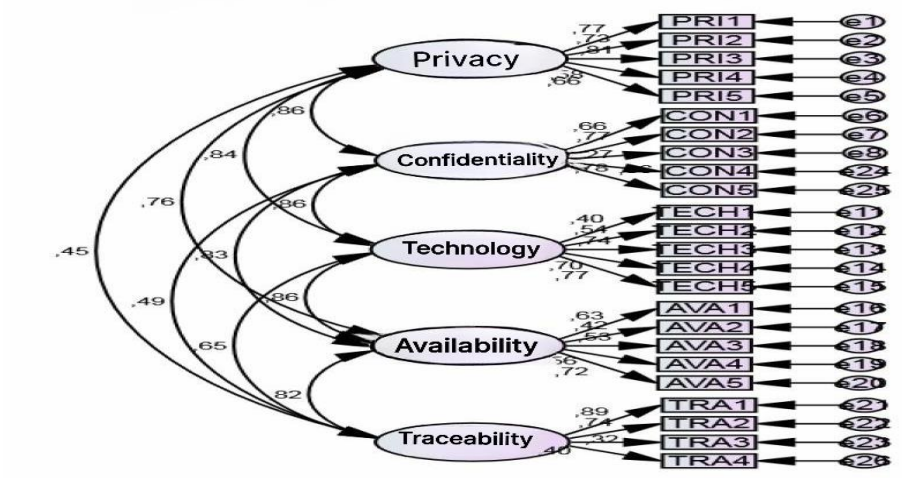

Figure No. 03: The Confirmatory factor analysis of cybersecurity dimensions
Source: Prepared by researchers based on Amos v26 results

The results of the indicators conforming to the cybersecurity form are summarized in the table as follows:

Table No. 06: Cybersecurity Form Conformity Indicators

The Indicator	The Recorded Value	Terms of acceptance of the form
Chi-Square (Cmin)	1063,526	Doesn't Prove
Standard Chi-Square (Cmin/df)	4,395	If between (2-5) indicated the quality of the form, and if between (1-2) indicated that the form had a good match.
Freedom Score (df)	242	(df≥0) A Particular Form
Significance Level (p-value)	.000	

Source: Prepared by researchers based on Amos v26 results

The Chi-Square indicator is one of the basic indicators for estimating the conformity of the theoretical model of the measurement model, its result: 1063,526 With a degree of freedom of 242, it is telltale at $p < 0.000$ that is below the level of 0.001. They are characterized as the most widespread and accurate when compared to other evidence, due to the fact that The Chi-Square (Chi^2) follows a normal distribution (95% of the data is concentrated within the field of acceptance, and 5% is the area of risk of error). However, there is no amount of Chi-Square or degree of freedom, which makes us sure that the result is good or not. Except by evaluating it by dividing The Chi-Square (Chi^2) by the degree of freedom. which gives us the standard, or relative, Chi-Square (Cmin/Df), which recorded a value of 4,395 and this result is considered very good, as it is confined between [5,2], in the sense that the measurement model may be highly compatible with the theoretical model. But Hair and others (Hair, et Al,1998) see this indicator as sensitive to the size of the sample, so not only is it recommended to use other indicators to match next to The Chi-Square (Chi^2).

Table No. 07: Cybersecurity Dimensions Model Conformity Indicators

The Indicator	The Recorded Value	Terms of acceptance of the form
Comparative Conformity Indicator (CFI)	0.942	CFI≥0.90 Better Match CFI = 1 Good Matching
Tucker Lewis indicator (TLI)	0.931	TLI≥0.90 Better Match TLI = 1 Good Matching
Incremental Conformity Indicator (IFI)	0.944	IFI≥0.90 Better Match IFI = 1 Good Matching

Source: Prepared by researchers based on Amos v26 results

In Table No. (07) we note that the value of the comparative conformity indicator (CFI) is equal to (0.942). This indicator measures the relative decrease of non-conformity, so that it is estimated according to the decentralized distribution of The Chi-Square (Chi^2) of the tested form compared to the basal or zero form,

which is a good value, within the area of acceptance of conformity estimated at 0.90 and above, allowing us to accept the form. As for the Tucker Lewis indicator (TLI), its value was: (0.931). This indicator compares the lack of conformity of the tested form with the base or zero form, which is a good value compared to the estimated pieces score by: 0.90 and above, which indicates that conformity is acceptable to the tested form, and for the IFI, its value is equal to (0.944). This indicator shows the extent to which the form studied for conformity exceeds the base or zero form, which is a good value, compared to the estimated pieces score of 0.90 and above for the form's acceptance.

Table No. 08: Conformity indicators of cybersecurity dimensions

The Indicator	The Recorded Value	Terms of acceptance of the form
Indicator of the root mean square error of approximation (RMSEA)	0,062	[0.05-0.08] Form Acceptance
Indicator of Average Standard Remains Square (SRMR)	0.0564	SRMR≥0.08 Better Match SRMR = 0 Complete Matching

Source: Prepared by researchers based on Amos v26 results

For Table Indicators No. (08): we find the value of the Indicator of the root mean square error of approximation (RMSEA) is equal to: (0.062). And The Indicator of Average Standard Remains Square (SRMR) is equal to: (0.0564) indicates that the form is in line with the data, the SRMR indicator is a measure of the average remains, and its near zero value indicates a good matching of the form. But The indicator of the root means square error of approximation (RMSEA), which corrects the rejection of the form by the Chi-Square indicator (Chi^2) with the large sample, is one of the most important indicators of matching quality. Its result in this form indicates that the form matches the data well because its value is within the limit for accepting conformity.

5.1) Convergent Sincerity of Cybersecurity Form:

Based on the results shown in chart No. (03) of the cybersecurity dimension model, the degree to which the cybersecurity dimensions are affected or saturated by the indicators or paragraphs expressed. Each of the values on each share from the underlying variables to each indicator or paragraph reflects the degree to which the underlying variable is saturated by these indicators or paragraphs. To compare these indicators in terms of the degree of saturation, or satisfaction of the underlying variable, we rely on standardized and non-standardized regressive weights, called "unstandardized" transactions of honesty or saturation on the underlying variable, as illustrated in the table of estimates, the following cybersecurity dimensions model:

Table No. (09): Cybersecurity Dimension Model Estimates

Saturations	Grade of Non-Standard	Grade of Standard (CR)	Standard Error (SE)	Significance Level
PRI1<---PRII	1,000			***
PRI2<--- PRII	,847	11,228	,075	***
PRI3<--- PRII	,903	12,720	,071	***
PRI4<--- PRII	,703	7,576	,093	***
PRI5<--- PRII	,768	8,763	,088	***
CON1<--- CONI	1,000			***
CON2<--- CONI	1,026	9,313	,110	***
CON3<--- CONI	1,131	9,470	,119	***
CON4<--- CONI	,350	3,619	,097	***
CON5<--- CONI	,438	4,738	,092	***
TECH1<--- TECHI	1,000			***
TECH2<--- TECHI	1,243	6,220	,200	***
TECH3<--- TECHI	2,252	5,125	,439	***
TECH4<--- TECHI	2,340	5,038	,464	***
TECH5<--- TECHI	2,775	5,115	,538	***
AVA1 <---AVAI	1,000			***
AVA2 <---AVAI	,395	4,674	,085	***
AVA3<--- AVAI	,541	6,194	,087	***
AVA4 <---AVAI	,609	6,290	,097	***
AVA5 <---AVAI	1,064	8,649	,092	***
TRA1<--- TRAI	1,000			***
TRA2<--- TRAI	,787	11,688	,067	***
TRA3<--- TRAI	,354	5 ,518	,064	***
TRA4<--- TRAI	,260	4,366	,059	***

Source: Prepared by researchers based on Amos v26 results

Table No. 09 shows us that the most satisfying variable of cybersecurity dimensions is indicator or paragraph No. (TECH5) in the sense that paragraph No. 5 of the technology used dimension (electronic payment card operations are always fast), reaching the non-standard degree of satisfaction (2,775) and a standard degree equal to 5,115. It is also clear that the least satisfactory indicators or paragraphs are paragraph (TRA4) in the area of tracking (the Bank's electronic documentation service leads to a person's ability to review and track the trajectory of electronic transfers, dates and timings), reaching a non-standard score of (260) and a standard score of 4,366. The rest of the paragraphs or indicators range from normative to non-normative degrees of satisfaction between these paragraphs.

Table No. (10): * Common variation and discrepancy derived * * for the concept of cybersecurity

	Privacy Respect	Data Confidentiality	Technology Used	Availability & Sustainability	Traceability
Privacy Respect	0.71	0.74	0.70	0.57	0.20
Data Confidentiality	0.74	0.56	0.74	0.68	0.24
Technology Used	0.70	0.74	0.63	0.74	0.42
Availability & Sustainability	0.57	0.68	0.74	0.57	.0.67
Traceability	0.20	0.24	0.42	0.67	0.59

Source: Prepared by researchers based on Amos v26 results

*** Common Variation:** the value of the correlation between factors multiplied by themselves.
*** * Extracted Variation:** the average arithmetic of multiple association.

We note from Table No. (10) on Common Variability Values and Extracted Variability Values that the variability values extracted for cybersecurity dimensions are above 0.40, all of which demonstrate the approximate veracity of the cybersecurity dimensions measure that it actually consists of five factors and twenty-four paragraphs or indicators.

5.2) Differentiated Honesty of Cybersecurity Dimensions Form:

We note from the cybersecurity model graph that the correlation factor between the five factors of the cybersecurity variable is below 0.90, that is, it indicates a fairly moderate correlation between the five factors (Privacy Respect, Data Confidentiality, Technology Used, Availability and Sustainability, Traceability) of the cybersecurity variable, thereby enhancing the differentiation of factors from each other in the sense of discriminatory sincerity. It is also evidence of discriminatory truthfulness that the values of divergence derived are higher than the values of common divergence between the dimensions of cybersecurity as in Table No. (10). Based on the foregoing, all indications of the cybersecurity scale are true to what has been developed to measure it.

Table No. (11): Stability and Honesty Test among Cybersecurity Factors

	CR	AVE	MSV	MaxR (H)	CONI	TECHI	AVAI	TRAI	PRII
CONI	0,718	0,695	0,741	0,799	0,731				
TECHI	0,775	0,585	0,746	0,811	0,855	0,834			
AVAI	0,710	0,674	0,746	0,735	0,826	0,864	0,765		
TRAI	0,820	0,534	0,676	0,845	0,492	0,653	0,822	0,760	
PRII	0,835	0,507	0,741	0,850	0,861	0,839	0,755	0,449	0,821

Source: Prepared by researchers based on Excel results

The Convergent Truthfulness of the Concept is Realized:

- The saturations are all indicative of that as mentioned.
- **Composite Stability (CR)** for each dimension is greater than **the Average Variability Extracted (AVE).**
- **The average variance extracted (AVE)** is greater than 0.5 per dimension.
- **The Differentiated Honesty** of the concept:
- where we found that: **The maximum common contrast square (MSV)** is smaller than **the average extracted contrast (AVE).**

6. View and analyze the results of cybersecurity dimensions:

- **Answer the question: What levels of response to customers' cybersecurity dimensions?**

After statistical processing, researchers found that:

Table No. 04: Arithmetic averages and standard deviations of cybersecurity axis vertebrae

No	Question	Arithmetic Average	Standard Deviation	Ranking	Degree
6	The bank is keen to give me a special confidential number for my e-card, since the day of delivery.	3.79	1.178	03	High
7	My data saved in the electronic payment card is content intact.	4.03	1,045	02	High
8	I care about protecting my personal data.	4.18	,996	01	High
9	The bank's electronic security performance affects my ATM selection.	3.64	1,228	05	Average
10	The Bank's security policy keeps my personal data confidential from posting or broadcasting.	3.79	1,177	04	High
	Privacy Respect	**3,88**	**,863**		**High**
11	The PIN of my e-payment card has a combination that makes it difficult to pirate.	3.55	1,050	05	Average
12	The Bank's electronic procedures oblige the electronic signature in all transactions.	3.97	,914	03	High
13	My e-transactions with the bank are completely confidential.	3.92	,985	04	High
14	The PIN of the electronic payment card is automatically exchanged for every given period.	4.24	,890	01	High
15	No one can access my data and my electronic information.	4.04	,841	02	High
	Data Confidentiality	**3,94**	**,640**		**High**
16	The Bank has modern, good and protected electronic technology equipment and devices.	3.92	,941	03	High

No	Question	Arithmetic Average	Standard Deviation	Ranking	Degree
17	The Bank automatically documents and records all my electronic transactions.	4.06	,826	01	High
18	The Bank's information systems and software operate accurately, in full harmony and complementarity.	3.81	1,073	04	High
19	I have a quick response to any e-card security and security issue.	3.43	1,196	05	Average
20	Electronic payment card operations always take place quickly.	4.03	1,300	02	High
	Technology Used	**3,84**	**,782**		**High**
21	The Bank's e-services are continuously available for 24 hours and every day of the week.	3.21	1,295	05	Average
22	The bank guarantees me the electronic flow of information about its services offered.	3.93	,856	03	High
23	Through my previous dealings with the electronic card, I often experienced a malfunction or dysfunction in the device or in the service provided.	4.04	,849	02	High
24	The Bank allows electronic access to my personal data to be reviewed or verified.	4.08	,939	01	High
25	The bank makes me feel the services I do, such as the withdrawn balance service.	3.48	1,078	04	Average
	Availability & Sustainability	**3,74**	**,703**		**High**
26	The Bank provides an instant freezing service for the electronic card if it is lost or stolen.	3.61	1,119	03	Average
27	I find it easy to change the bank to my PIN when I have to.	3.33	1,046	04	Average
28	The Bank adopts electronic documentation service for all data related to electronic card operations to achieve the security and tracking of electronic transactions.	3.85	,907	02	High
29	The Bank's e-documentation service leads to my ability to review and track electronic transfers, dates and timings.	3.86	,829	01	Average
	Traceability	**3,66**	**,727**		Average

Source: Prepared by researchers based on SPSS V26 data.

The results of the statistical analysis gave the results of the cybersecurity dimensions divided into five paragraphs as follows:

6. Privacy Respect: Questions from 06 to 10

According to the results of the statistical analysis, respect for privacy on the cybersecurity side is second only to the confidentiality dimension, where the

overall arithmetic average of the dimension was (high): 3.88 with a standard deviation of: 863. The ninth question ranked first with an average calculation of: 4.18 with a standard deviation of: 996 interrogators consider that attention to the protection of their personal data is very important.

6.1) Data Confidentiality: Questions from 11 to 15

The results from the statistical analysis programme indicate that the data confidentiality dimension was at the forefront of cybersecurity, as the arithmetic average of this dimension was (high) and was: 3.94 With a standard deviation of:, 640 Question No. 15 included (Electronic Payment Card PIN automatically replaced every given period), the highest arithmetic average of 4.24 with a standard deviation of: 890 interrogators consider that changing their electronic card's PIN from period to time is a good mechanism or way to ensure the confidentiality of their PIN and protect their personal data from espionage, sabotage, theft, etc.

6.2) Technology Used: Questions from 16 to 20

The results of the statistical analysis showed that cybersecurity in the dimension of the technology used was the third after both data confidentiality and after respect for privacy with a general arithmetic average (high) calculation of: 3,84 With a standard deviation of: 782, the average arithmetic of question 18, which stipulated (the Bank automatically documents and records all my electronic transactions), reached an average arithmetic of: 4.06 With standard deviation:, 826 the bank's authentication process automatically allows the consumer recourse to it to know all its electronic operations and in the sense that it is considered as both a reference and a guide, which is very important in electronic processes conducted by electronic cards.

6.3) Availability & Sustainability: Questions from 21 to 25

Results from the Statistical Analysis Programme show that the level of availability and sustainability in cybersecurity was (high) with the arithmetic average of the dimension: 3.74 With a standard deviation of:, 703 and thus ranked fourth in the dimensions of cybersecurity, the arithmetic average of question No. 25 was the highest: 4.08 With standard deviation:, 939 Where interrogators consider that the Bank provides electronic access to customers' personal data to be reviewed or verified, the provision of such service is very important, for example the review of the balance in the account or the verification of certain electronic transactions.

6.4) Traceability: Questions from 26 to 29

What can be seen from the results of the statistical analysis is that The Traceability on cybersecurity has the weakest ratio with the arithmetic average: 3.66 degrees (average) with a standard deviation of: 727. The sample response to question 30, which stipulated (the Bank's e-documentation service leads to my ability to review and retrace the trajectories of electronic transfers, dates and timings), averaged an account (high) of: 3,86 standard deviations amounting to: 829 because the responder considers that this service allows him to track the

trace of all his electronic transfers and traces even knowing their dates and timing. Using the ordinal arithmetic averages of cybersecurity dimensions, we find the following:

Table No. 05: Arrangement of The Arithmetic Averages and Deviations of Cybersecurity Dimensions

The Deviations	Arithmetic Average	Degree	Standard Deviation	Ranking
Privacy Respect	3,88	High	,863	02
Data Confidentiality	3,94	High	,640	01
Technology Used	3,84	High	,782	03
Availability & Sustainability	3,74	High	,703	04
Traceability	3,66	Average	,727	05

Source: Prepared by researchers based on SPSS V26 data.

7. Conclusion

After extensively addressing the dimensions of cybersecurity in the Algerian banking environment, and in order to develop a theoretical framework for the most important concepts associated with these dimensions, the study focused its field aspect on proving the validity of the hypotheses formulated earlier by using the questionnaire as the main tool for field study and analysis of its results. Thereafter, a set of conclusions was reached in the theoretical and applied parts, the most important of which will be reviewed in the following points:

- The Scale Form is highly compatible with The Theoretical Form.
- The discrepancy values extracted for cybersecurity dimensions obtained are above 0.40. Thus, it proves the approximate truthfulness of the cybersecurity dimension scale, so we can say that it actually consists of five factors: (Privacy Respect, Data Confidentiality, Technology Used, Availability and Sustainability, Traceability).
- The cybersecurity model is devoid of illogical correlation values, being the correct single override (01).
- The ratio of saturation or honesty between the five cybersecurity factors and its vertebrae or indicators is good and encouraging, most of which exceeded 0.40 with morale levels (p-value = 0.000).
- The correlation factor between the five factors of the cybersecurity variable is below 0.90. that is to say, somewhat mild interdependence, which promotes differentiation of factors from one another in the sense that they enjoy discriminatory sincerity.

Based on the findings we can providing a set of proposals:

- ❖ This study seeks to introduce an integrated conceptual framework that can be used in the cybersecurity performance of banking digital services.
- ❖ We propose that Algeria's banking system adopt the proposed cybersecurity model with its five components (Privacy Respect, Data Confidentiality, Technology Used, Availability and Sustainability, and Traceability) as

necessary elements in the production process of digital banking services to ensure their safety and enjoyment of all quality characteristics.

- ❖ We recommend increased security tools with field measures and actions based on the five dimensions of cybersecurity in digital banking services to enhance the customer's level of confidence in them.
- ❖ We advise the Bank to establish a mechanism to assess the performance of cybersecurity and the customer's level of confidence in its digital services.
- ❖ Banking must recognize risk levels to consider and work to resolve as they negatively affect customers for their use of digital banking services.
- ❖ The need to introduce information systems and communication networks with ISO standards.

8. Reference List:

Mohamed Bozian Teighza, Recent Trends in Estimating the Honesty and stability of Measuring Instrument Degrees, Journal of Psychological and Educational Sciences, Martyr Hamah Lakhdhar University, El Oued State Algeria, vol. 04 Issue (01), March 2017, p. 10.

Thaib bin Ayad Al-Qahtani, Information Security, King Abdulaziz City of Science and Technology Publishing House KACST, Riyadh, Saudi Arabia, 2015, pp. 91-100.

Mona Al-Ashqar Jabbour, Mahmoud Jabbour, Personal Data and Arab Laws, Studies and Research of the Arab Center for Legal and Judicial Research (Information Security and Legal Security), Beirut, Lebanon, 2019, p. 18.

Mona Abdullah Al Samhan, Requirements for Cybersecurity of Management Information Systems at King Saud University, Journal of Faculty of Education, Mansoura University, No. 11, July 2020, p. 12.

Report of the International Telecommunication Union of the United Nations, 2011, website: (http://www.itu.int), date of view: 28-10-2024, at 22:40.

Osama Husamuddin, Introduction to Cybersecurity 0.2, Faculty of Computer Science and Engineering, Cisco Academy, 2017, p. 10.

Marizeq Adman, Imad Boukalashi, Information Security under Electronic Commerce, referring to the cases of Tunisia and Algeria, made an intervention at the fourth International Scientific Forum on the modernization of the payment system in Algerian banks and the problem of accreditation of electronic commerce in Algeria. Presentation of International Experiences, published, University Centre Khemis Miliana University, Algeria, 26-27 April 2011, p. 4.

Saeed Ziosh, Electronic Commerce and Consumer Privacy Protection Mechanisms of Algeria, Herodotus Journal of Humanities and Social Sciences, Barika, Batna, Algeria, vol. 7, No. 25, 2023, p. 10.

Law No. 18-04, on the General Rules on Mail and Electronic Communications of Algeria, of 24 Sha 'ban 1439, corresponding to 10 May 2018, article 10, C.R.C.C, Title I, Section II, No. 27, issued on: May 13, 2018, p. 7.

Farida Hammoudi, Information Security in Algeria between technological developments and the weakness of the digital environment of the banking field, Generation Magazine of In-depth Legal Research, No. 41, 2020, p. 91.

Amos Olushola Michael, **The Effect of Electronic Banking on Bank Performance in Nigeria**, **European Journal of Business and Management,** Vol 12, N 26, 2020, P 79.

Daniel Ventre, **Cyberattaque et cyberdéfense,** La Voisier, Paris, 2011, P 103.

Douwe Korff, **Cyber Security Definitions** - a selection, 2015, P 1.

Kritika Law, **Impact of Perceived Security on Consumer Trust in Online Banking,** Auckland New Zealand, 2007, P 22.

Qais Amiri, Tahaer Majali, Damaithan Almajali, Abdalrazzaq Aloqool, Jassim Ahmad Al-Gasawneh, **Explore the Relationship Between Security Mechanisms and Trust in E-Banking: A Systematic Review**", Annals of R.S.C.B, ISSN: 1583-6258, Vol 25, N 6, 2021, PP 17083-17093.