HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

Peer-Reviewed Journal
Indexed at: NSP - SJIF
Impact Factor 2022 = 4.91

RESEARCH TITLE

THE IMPACT OF INFORMATION SECURITY ON THE OF INFORMATION SYSTEMS USERS' CONFIDENCE
A field study in private banks in Saudi Arabia

Jamal Ahmed Radman[1] **Sabaa Hatem Shafy**[2]

[1] Maintenance Supervisor , Gulf Medical Company Limited. Jeddah-Saudi Arabia.
Email: jamal.radman@gmail.com

[2] Principal Deputy, Cordoba National Schools. Jeddah-Saudi Arabia.
Email: sabaashafy@gmail.com

HNSJ, 2024, 5(1); https://doi.org/10.53796/hnsj51/47

Published at 01/01/2024 **Accepted at 05/12/2023**

Abstract

Within the context of private banks in Saudi Arabia, the purpose of this study is to investigate the influence that information security has on the users' trust in their ability to use information systems. For the purpose of this study, a quantitative methodology is utilised, and a survey questionnaire is utilised to collect data from 384 individuals who use private banks. Awareness, policy compliance, behaviour, and management are the four aspects that are utilised in the course of the research to quantify information security. The study also used a single construct to quantify the level of confidence possessed by users. The hypotheses are put to the test through the use of correlation and regression analyses in this study. Approximately 52.7% of the variation in users' confidence may be attributed to information security, as demonstrated by the findings, which indicate that there is a positive and significant association between information security and users' confidence. In addition, the findings indicate that the management of information security is the most crucial aspect of information security, followed by awareness, compliance with policies, and behaviour. A comparison is made between the findings of this study and those of prior studies, and some recommendations are offered for private banks as well as for future research.

Key Words: Information security, Users' confidence, Private banks, Saudi Arabia.

1. Introduction

When it comes to information systems, information security is an essential component since it safeguards the confidentiality, integrity, and availability of data and resources against unauthorised access, use, modification, or destruction (Sharma et al., 2021). There is also a correlation between information security and the trust of users of information systems, who are dependent on the systems to carry out a variety of activities and duties (Gilman Ranogajec & Badurina, 2021). It is possible to describe the level of confidence that users have in information systems as the degree to which they have trust and contentment in the outputs of those systems (Gilman Ranogajec & Badurina, 2021). The confidence of users can have an effect on their behaviour, including the frequency and length of system usage, the readiness to share and reveal information, and the degree to which they comply with security policies and procedures.(Sharma et al., 2021).

However, information security is not a static or absolute concept, but rather a dynamic and relative one, that depends on various factors, such as the type and level of threats, the security measures and controls implemented, the user awareness and education, and the organizational and environmental context (ISO/IEC 27018:2019). Therefore, it is important to understand how information security affects users' confidence in different settings and scenarios, and what are the factors that enhance or diminish users' confidence.

One of the settings that is particularly relevant and challenging for information security and users' confidence is the banking sector, especially in the context of Saudi Arabia. The banking sector is a vital and strategic sector for the national economy, and it faces various information security risks, such as cyberattacks, fraud, identity theft, and data breaches (Alzahrani, A., & Alharbi, A., 2023). The banking sector also relies heavily on information systems to provide various services and products to customers, such as online banking, mobile banking, ATM, and POS (Alshammari, M., & Alhussain, H., 2021). Therefore, the confidence of banking customers in the information systems and their security is essential for the success and competitiveness of the banking sector.

However, the banking sector in Saudi Arabia has some unique characteristics and challenges that may affect information security and users' confidence. For example, Saudi Arabia is a conservative and religious society, where Islamic law and values play a significant role in shaping the culture and norms of the people (SABB, 2023). This may affect the perception and attitude of banking customers towards information security and privacy, as well as their expectations and preferences for banking services and products.

Moreover, Saudi Arabia is undergoing a rapid and ambitious transformation process, known as Vision 2030, which aims to diversify the economy, modernize the society, and enhance the quality of life (SABB, 2023). This may create new opportunities and challenges for the banking sector, as well as for information security and users' confidence.

As a result, the primary purpose of this research is to investigate the influence that information security has on the trust of individuals who utilise information systems in the banking industry in Saudi Arabia. To be more specific, the research will carry out a field study at private banks in Saudi Arabia, which are often regarded as the most innovative and well-established institutions in the country (SABB, 2023). The investigation will make use of a mixed-methods approach, which will combine qualitative and quantitative methods of data collecting and analysis. These methods will include but are not limited to questionnaires, interviews, and observations (Sharma et al., 2021). A theoretical framework that is based on a literature study of important ideas and models will also be utilised in the research. Some examples of these concepts and models include information security, users' confidence, trust, satisfaction, and behavioural intention.

The expected contributions of this research are as follows:

- It will provide a comprehensive and in-depth understanding of the impact of information security on users' confidence in the banking sector in Saudi Arabia, and the factors that influence this relationship.

- It will offer practical and useful recommendations and guidelines for improving information security and users' confidence in the banking sector in Saudi Arabia, and for addressing the current and future challenges and opportunities in this domain.
- It will enrich and advance the academic and scientific knowledge and literature on information security and users' confidence, especially in the context of Saudi Arabia and the Middle East region, which are under-researched and under-represented in this field.

Following is the structure of the remaining parts of this paper: In the second section, a literature review is conducted on the topic of information security and the confidence of users. Additionally, the theoretical framework and study hypotheses are presented. A description of the study methodology is provided in Section 3, which covers topics such as the research design, data collecting, and data analysis. The outcomes of the data analysis and the hypothesis testing are reported and discussed in Section 4, which is the fourth section. In the fifth and last section of the paper, the limits of the study as well as the recommendations for further research are discussed.

Problem Statement

There are many different information security dangers that the banking industry faces, including cyberattacks, fraud, identity theft, and data breaches. Being a crucial and strategic sector for the national economy, the banking sector is also vulnerable to these risks. The banking industry is also extensively dependent on information technologies in order to deliver a wide range of services and products to consumers. These include internet banking, mobile banking, automated teller machines, and point-of-sale terminals. As a result, the confidence of banking clients in the information systems and the security of those systems is crucial for the success and competitiveness of the banking sector (BCG, 2023).

As a result, there is a dearth of understanding on how the confidence of users is affected by information security in a variety of settings and circumstances, as well as the elements that either increase or decrease the trust of users. In addition, there is a dearth of empirical research that investigates the influence of information security on the confidence of customers in the banking industry, particularly in the setting of Saudi Arabia. The gap in the literature and practise on the influence of information security on the trust of information systems users in the banking industry in Saudi Arabia is the primary issue that this research intends to solve. This research tries to fill this gap. The significance of this issue lies in the fact that it has an impact not only on the efficiency and profitability of the banking industry, but also on the contentment and commitment of the customers' banking relationships. Furthermore, this issue is pertinent and contemporary since Saudi Arabia is currently in the midst of a quick and ambitious transformation process known as Vision 2030. The objective of this process is to modernise the society, diversify the economy, and improve the quality of life. There is a possibility that this process may bring forth new opportunities and problems for the banking industry, as well as for the protection of information and the confidence of users.

2. Literature review

The goal of information security is to prevent data loss, misuse, alteration, or disclosure by implementing and maintaining appropriate organisational, legal, and technological safeguards. Network and infrastructure security, data security, application security, and cybersecurity are all subfields that fall under this umbrella term. Network and infrastructure security ensures that a system or network's physical and logical components are safe from harm. Data security addresses how a system or network stores, processes, or transmits data. Finally, cybersecurity protects a system or network from external threats and malicious attacks. (Whitman, M. E., & Mattord, H. J., 2018). Data that is vital to the functioning and success of a business, such as customer account information, financial records, or intellectual property, must be protected against unauthorised access while still maintaining its integrity and availability (Stallings, W., & Brown, L., 2018). Information is one of the most precious assets in the digital era, and unauthorised parties may readily access, copy, or alter it. Therefore, information security is crucial for every company that gathers, processes, stores, or transmits information (Pfleeger et al., 2015).

Protecting the data and transactions of stakeholders, customers, and workers against cyber dangers such phishing, malware, ransomware, denial-of-service attacks, data breaches, identity theft, fraud, and money laundering is the particular goal of information security in banks. Information and financial transactions' privacy and security, along with the credibility and bottom line of financial institutions, are all at risk from these dangers (Dhillon, G., & Backhouse, J., 2001). Consequently, financial institutions must establish robust information security protocols. These protocols should include the following: encryption, authentication, firewalls, antivirus, intrusion detection and prevention, and risk assessment and management (Alawneh et al., 2013).

When people are confident in a system or platform, such a website, app, or gadget, it means they are satisfied with the level of security and privacy that the system or platform provides for their information and transactions. The user's perception of the system or platform's quality and performance is impacted by factors like design, usability, functionality, and reliability. Additionally, the user's expectation and evaluation of the system or platform's outcome are affected by factors like the user's perception of the risks and benefits associated with using the system or platform (Kim et al., 2008). Because it impacts the user's propensity to use the system or platform, how often they use it, and whether or not they promote it to others, user confidence is critical to the platform's or system's success in attracting and retaining users (Alalwan et al., 2016).

User confidence is influenced by the implementation and perception of information security, which may have both good and bad effects on user confidence. Hence, there is a link between the two. Information security, on the one hand, may boost users' confidence by reducing their perceived risk and uncertainty when using the system or platform and increasing their sense of privacy and security through protection, assurance, and transparency (Lee, M. C., 2009). In contrast, users' trust may be eroded by information security measures that are overly complicated, restricting, and inconvenient. This can make users feel less in control and freedom while also increasing the perceived effort and expense of utilising the system or platform (Liao, Z., & Cheung, M. T., 2002). In order to reach the highest degree of user confidence, information security must strike a balance between security and usability while also taking into account the tastes and expectations of various users (Furnell, S., 2005).

In order to keep data and systems safe and usable, information security and user confidence are interdependent ideas. The term "information security" is used to describe the procedures and policies put in place to safeguard data from being misused, altered, accessed, transferred, or destroyed, regardless of its location (ISO/IEC 27004:2016). Conversely, user confidence is defined as the extent to which end users are satisfied with the privacy and security of their data and systems (Fruhlinger, J., 2020).

A number of theories and models attempt to explain the connection between information security and users' confidence. For example, one model proposes that users' perceptions of a system's usefulness and ease of use play a role in their acceptance and usage of the system. Another model, the trust model, posits that users' perceptions of a system's trustworthiness and risk impact their confidence and trust in the system. Lastly, the protection motivation theory posits that users' perceptions of the severity and vulnerability of threats, along with their perceived response, influence their motivation and behaviour in safeguarding their information and transactions (Li, Y., 2012). Perceived utility, trustworthiness, risk, benefit, attitude, intention, and behaviour are some of the cognitive, affective, and behavioural elements that theories and models imply impact information security and users' confidence. These factors can differ for each user based on their characteristics, context, and situation (Venkatesh et al., 2003). Cheng et al., Sharma et al. (2021), and Gilman Ranogajec and Badurina (2021) are a few examples of the empirical investigations that back up these ideas and models (2012). Evidence from these studies suggests that information security interventions—like digital nudging, framing, and priming—can influence users' confidence and behaviour in various contexts, including cybersecurity, social media, and smartphone security. This is due to the fact that these interventions change users' perceptions and evaluations of information security, as well as their confidence factors (Acquisti et al., 2015)

The confidence and happiness of customers depend on the banking and financial industry's commitment to protecting their personal information and financial transactions. Data security, application security, cybersecurity, and network and infrastructure security are all subfields of information security that work together to protect the privacy, authenticity, and accessibility of sensitive information. The goal of information security in financial institutions is to prevent loss, misuse, alteration, or destruction of data due to malicious software, accidental deletion, theft of personal information, fraud, or other forms of electronic crime. Encryption, authentication, firewalls, antivirus, intrusion detection and prevention, risk assessment and management, security awareness and training, and compliance with legislation and standards are all essential components of an efficient information security strategy for banks. Because it impacts the interests and rights of everyone working in the banking and financial sector, information security in banks is a strategic, ethical, and technically complex problem.

3. Methodology

Studying how private Saudi Arabian banks' information system users' confidence is affected by information security is the primary goal of this research. The study uses quantitative methods of data collecting and analysis to reach this objective.

Using a poll of Saudi Arabian private bank personnel who often interact with IT systems is the quantitative technique. There are two parts to the survey. Part one asks basic personal questions including age, gender, education, occupation, and years of experience. Part two asks more in-depth questions regarding the respondents' experiences and opinions. In the second part, we ask respondents to rate their level of trust in utilising information systems and how they feel about information security on a five-point Likert scale. The respondents' level of agreement was measured using a 5-point Likert scale, where 1 indicates strongly disagree and 5 indicates strongly agree. The current investigation necessitated adjustments to each variable's items.

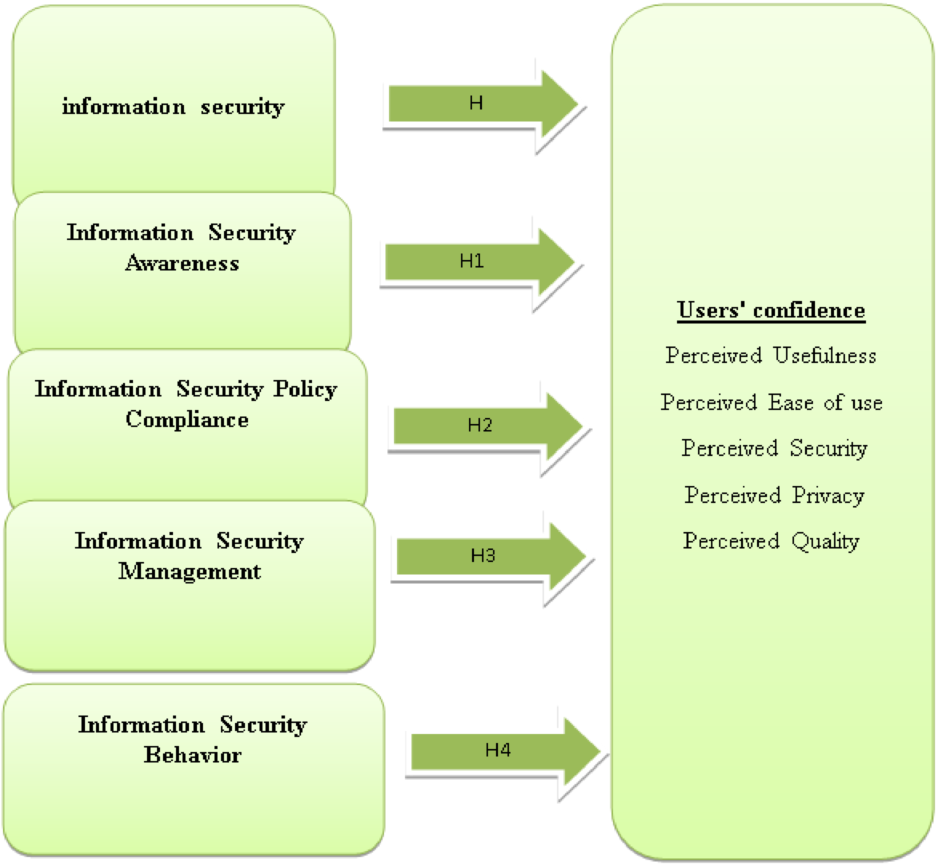
Previous research on user confidence and information security (Alzamil, Zakarya., 2018; Elamin, Bushra., 2016; Tahani et al., 2023; Almaiah et al., 2022) served as inspiration for the survey questions (Humaidi, 2018).

Data is collected and analysed using SPSS software after the survey is circulated online through email and social media sites. Statistical methods such as multiple regression, correlation, validity and reliability testing, and descriptive statistics are all part of the data analysis process.

Information security and user confidence are the primary research factors in this study. Data protection is the one that doesn't change. As a measure of how happy and trusting users are with the information systems they use, users' confidence serves as the dependent variable (Cheng et al., 2021).

There are a lot of different ways to measure and assess both variables. There are four parts to information security: knowing how to protect sensitive data, following established policies, acting responsibly, and keeping track of everything (Cram et al., 2017). Perceived utility, usability, security, privacy, and quality are the aspects of trust that people have in a product (M. Dhingra and R. K. Mudgal, 2019).

Following figure no.1 represent the research model



The research's independent variable is information security, while the dependent variable is consumers' confidence, as seen in the above figure. Acknowledgment, policy compliance, behaviour, and administration are the four pillars of information security. Perceived utility, perceived simplicity of use, perceived safety, perceived privacy, and perceived quality are the five facets that make up users' trust. Information security boosts users' confidence, which is the research's major hypothesis (H), as seen in the figure.

Some previous studies that support this figure are:

Data security is related to one's personality, according to research by Kraus et al. (2017). Using smartphone use as an example, they looked at how people's psychological needs can motivate them to take security and privacy measures.

Digital nudging and its effects on information security behaviour are investigated by Sharma et al. (2021). In order to manipulate consumers into taking risks in a phishing situation, they employ framing and priming strategies.

The trust that social media users have in the safety and privacy of their data is quantified by Cheng et al. (2021). They poll users on how well social networking sites work, how easy they find it to use, and how concerned they are about their privacy and security.

The main hypothesis of your research is:

H: Information security has a positive impact on users' confidence.

This hypothesis can be tested by examining the relationship between information security and users' confidence, using the dimensions of both variables as indicators. The sub-hypotheses for your research are:

H1: Information security awareness has a positive impact on users' confidence.

H2: Information security policy compliance has a positive impact on users' confidence.

H3: Information security behavior has a positive impact on users' confidence.

H4: Information security management has a positive impact on users' confidence.

4. Results and findings

4.1. Scale Validity and Reliability:

The internal consistency test was run to ensure the reliability of the study instrument (questionnaire). The results are shown in table No. (1) below. They demonstrate that the Cronbach's Alpha value was greater than 60% for every section of the questionnaire.

All things considered, this proves that the research instrument is quite stable and trustworthy.

Table no.1: Reliability Statistics

Variable	Cronbach's Alpha	N of Items
Information security awareness	0.872	6
Information security policy compliance	0.601	6
Information security behavior	0.789	6
Information security management	0.729	6
Users' confidence	0.878	30
Total	0.821	45

4.2. Respondent's Demographic statistics

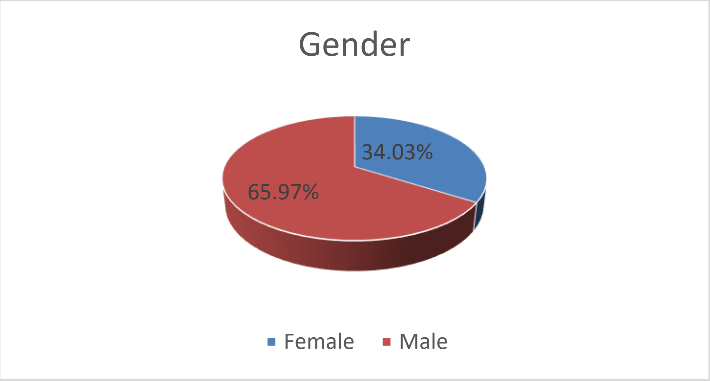
The demographics questions included gender, age, education, and experience.

Gender

The results of the study members responses about the gender as showing in the below table indicate that “Male” represents of 65.97%. While “Females” represents only 34.03%.

Table no.2: Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	131	34.03	34.03	40.03
	Male	254	65.97	65.97	100.0
	Total	385	100.0	100.0	

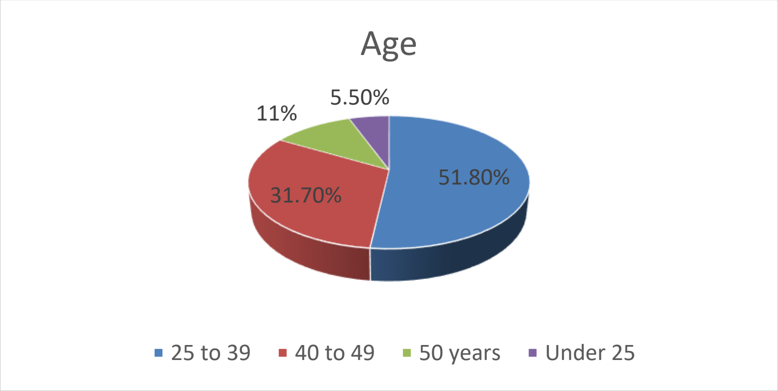


Age

The results of the study members responses about the age as showing in the below indicate that responders age between 25-39 years came in the first place by 51.8% of total number of responders, whereas the age under 25 years came in the last place by only 5.5% of total number of responders. who represent 32.4%. While comes in the second place the age category between 40-49 years old by 31.7% of total number of responders, which represent 22.5%.

Table no.3: **Age**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	25 to 39	200	51.8	51.8	51.8
	40 to 49	122	31.7	31.7	83.5
	50 years	42	11.0	11.0	94.5
	Under 25	21	5.5	5.5	100.0
	Total	385	100.0	100.0	

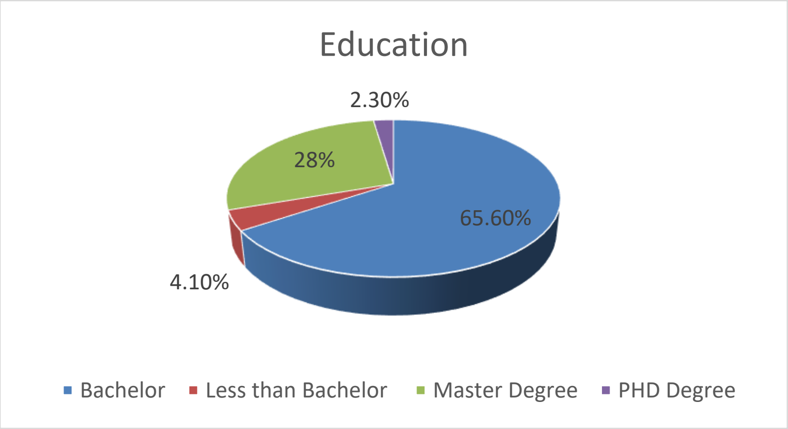


Education

he results of the study members responses about the education level as showing in the below table indicate that the Bachelor holders came in the first place by 65.6% of the total number of the study sample, and Master degree holders came in the second place by 28% of the total number of the study sample.

Table no.4: **Education**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bachelor	253	65.6	65.6	65.6
	Less than Bachelor	16	4.1	4.1	69.7
	Master Degree	108	28.0	28.0	97.7
	PHD Degree	8	2.3	2.3	100.0
	Total	385	100.0	100.0	

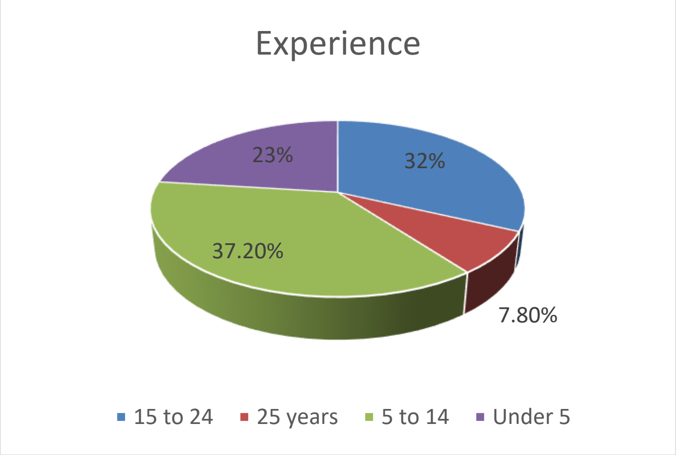


Experience

The results of the study members responses about the years of experience as showing in the below table indicate that the category from 5 to 14 years of experience came in the first place by 37.2% of total sample of the study, and the category from 14 to 24 years of experience came in the second place by 32 % of total sample of the study, whereas the category 25 years of experience and above came in the last place by only 7.8% of total sample of the study.

Table no. 5: **Experience**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	15 to 24	123	32	32.1	32.1
	25 years	30	7.8	7.8	39.9
	5 to 14	143	37.2	37.2	77.1
	Under 5	89	23	22.9	100.0
	Total	385	100.0	100.0	



4.3. Hypothesis Testing

Sub-hypothesizes Testing

H1: Information security awareness has a positive impact on users' confidence.

Table no.6: **Model Summary**

R	R Square	Adjusted R Square	Std. Error of the Estimate
.403	.163	.159	.581

The independent variable is Information Security Awareness.

Table no.7: **ANOVA**

	Sum of Squares	df	Mean Square	F	Sig.
Regression	14.186	1	14.186	41.959	.000
Residual	73.025	216	.338		
Total	87.211	217			

The independent variable is Information Security.

Coefficients Table no.7:

	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	Sig.
Information Security Awareness	.436	.067	.403	6.478	.000
(Constant)	2.630	.260		10.118	.000

The above tables show that the Correlation value between Information Security Awareness and users' confidence is 0.403 which indicates that the relation is moderate positive correlation. The regression test shows that the Adjusted R square is 0.159 which means that the Information Security Awareness interprets about 15.9% of users' confidence in private banks in Saudi Arabia, And the Anova test table shows that F value for the test reached 41.959 which is very high that indicate that the test is significant and can be relied on. And since the significant value for F test reached 0.000 < 5% that means this test is Significant at 5%. Therefore, the first sub-hypothesis is partially accepted.

H2: Information security policy compliance has a positive impact on users' confidence.

Model Summary Table no.8:

R	R Square	Adjusted R Square	Std. Error of the Estimate
.450	.203	.199	.567

The independent variable is Information security policy compliance.

ANOVA Table 9:

	Sum of Squares	df	Mean Square	F	Sig.
Regression	17.693	1	17.693	54.974	.000
Residual	69.518	216	.322		
Total	87.211	217			

The independent variable is Information security policy compliance.

Coefficients Table 10:

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
Information security policy compliance t	.645	.087	.450	7.414	.000
(Constant)	1.591	.367		4.340	.000

The above tables show that the Correlation value between Information security policy compliance. users' confidence which indicates that the relation is moderate positive correlation. The regression test shows that the Adjusted R square is 0.199 which means that the Information security policy compliance interprets about 19.9% of users' confidence in private banks in Saudi Arabia, And the Anova test table shows that F value for the test reached 54.974 which is very high that indicate that the test is significant and can be relied on. And since the significant value for F test reached 0.000 < 5% that means this test is Significant at 5%. Therefore, the second sub- hypothesis is partially accepted.

H3: Information security behavior has a positive impact on users' confidence.

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.534	.285	.282	.537

The independent variable is Information security behavior.

ANOVA

	Sum of Squares	Df	Mean Square	F	Sig.
Regression	24.894	1	24.894	86.286	.000
Residual	62.317	216	.289		
Total	87.211	217			

The independent variable is Information security behavior.

Coefficients

	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	Sig.
Information security behavior	.556	.060	.534	9.289	.000
(Constant)	2.164	.232		9.326	.000

The above tables show that the Correlation value between Information security behavior and users' confidence is 0.534 which indicates that the relation is good positive correlation. The regression test shows that the Adjusted R square is 0.282 which means that the Information security behavior interprets about 28.2% of users' confidence in private banks in Saudi Arabia, and with an effect coefficient of 0.556. And the Anova test table shows that F value for the test reached 86.286which is very high that indicate that the test is significant and can be relied on. And since the significant value for F test reached 0.000 < 5% that means this test is Significant at 5%. Therefore, the third sub-hypothesis is accepted.

H4: Information security management has a positive impact on users' confidence.

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.543	.295	.291	.534

The independent variable is Information security management.

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Regression	25.688	1	25.688	90.190	.000
Residual	61.523	216	.285		
Total	87.211	217			

The independent variable is Information security management.

Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
Information security management	.519	.055	.543	9.497	.000
(Constant)	2.282	.215		10.621	.000

The above tables show that the Correlation value between Information security management and users' confidence is 0. 543 which indicates that the relation is good positive correlation. The regression test shows that the Adjusted R square is 0. 291 which mean that the Information security management interprets about 29.1% of users' confidence in private banks in Saudi Arabia, And the Anova test table shows that F value for the test reached 90.190 which is very high that indicate that the test is significant and can be relied on. And since the significant value for F test reached 0.000 < 5% that means this test is Significant at 5%. Therefore, the fourth sub- hypothesis is accepted.

Main Hypothesis Testing

H: Information security has a positive impact on users' confidence.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.737[a]	.542	.527	.43591

a. Predictors: (Constant), Awareness, Policy Compliance, Behavior, and Information Security Management

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	47.307	7	6.758	35.565	.000[b]
	Residual	39.904	210	.190		
	Total	87.211	217			

a. Dependent Variable: Users' confidence

b. Predictors: (Constant), Awareness, Policy Compliance, Behavior, and Information Security Management.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.386	.303		1.275	.204
	Awareness	-.068-	.067	-.063-	-1.022-	.308
	Policy Compliance	.079	.083	.055	.949	.344
	Behavior	.149	.069	.143	2.162	.032
	Compatibility	.063	.066	.065	.950	.343
	Information Security Management.	.330	.095	.292	3.462	.001

a. Dependent Variable: Users' confidence

The above tables show that the Correlation value between all Information Security Diminutions and users' confidence of using the information systems in private banks in Saudi Arabia is 0.737 which indicates that the relation is strong positive correlation. The regression test shows that the Adjusted R square is 0. 527 which mean that all proposed Information Security Diminutions interpret about 52.7% of users' confidence of using the information systems in private banks in Saudi Arabia._And the Anova test table shows that F value for the test reached 35.565 which is very high that indicate that the test is significant and can be relied on. And since the significant value for F test reached 0.000 < 5% that means this test is Significant at 5%. Therefore, the main research hypothesis is accepted.

5. Discussion results and conclusion

Information security and customer trust in Saudi Arabia's private banking sector are positively correlated, according to this study's findings. Users' trust was shown to be moderately affected by each of the four aspects of information security: awareness, policy compliance, behaviour, and management. Among these factors, awareness, policy compliance, and information security behaviour had the most explanatory power and correlation, while information security management topped the list. Users have higher faith in private banks' information systems when they believe those systems are well-managed and that prudent rules and procedures are in place to safeguard customers' personal information and financial assets. In addition, the results demonstrate that users' confidence is significantly affected by information security across all four dimensions, supporting the main research hypothesis that information security plays a substantial role in this regard.

These results are in line with other research that has looked at the correlation between user trust and information security in various settings. As an example, a study conducted by Zhang, J., Luximon, Y., & Song, Y. (2019) titled "Role of Consumers' Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness" discovered that users' continuous use of mobile payment services was positively impacted by perceived security, a concept closely related to information security. In a similar vein, the research conducted by Hamakhan, Y. T. M. (2020) "The effect of individual factors on user behaviour and the moderating role of trust: an empirical investigation of consumers' acceptance of electronic banking in the Kurdistan Region of Iraq" revealed that trust played a mediating role in the relationship between users' acceptance of electronic banking services and individual factors like perceived security, usefulness, and ease of use. The results of these research point to the importance of consumers' perceptions of information security when it comes to their use of online banking and other financial services. There have been previous studies that have looked at the same or comparable issues, but this one found different conclusions. One such research is "Banking's Cybersecurity Blind Spot—and How to Fix" (Grasshoff et al., 2018). It stated that many financial institutions have not adequately addressed cyber risk and that they should change their business models to include cybersecurity in the same category as credit, counterparty, and compliance risks. This research seems to suggest that banks' present data security measures aren't enough to keep customers happy and confident. In a similar vein, research by Sabau, C. (2022) titled: "5 Ways in Which Banks Secure Their Data" posits that, to safeguard their data from cyberattacks or unauthorised access, banks ought to institute a number of data security best practises, including authentication, encryption, monitoring, and backup. According to their research, banks might do a better job of protecting their customers' personal information, and customers might not be completely aware of the risks they face while using the banking system.

Some suggestions for future study and private banks in Saudi Arabia may be derived from the results and comparison with prior studies. Since management, behaviour, and policy compliance are the three most important aspects affecting customers' trust in private banks, it is advised that these institutions maintain and enhance their investments in information security. They need to explain and teach their customers on the pros and cons of utilising their systems, as well as how to safeguard their information and possessions. More empirical investigations should be undertaken to confirm and expand upon the results of this study, as well as to investigate other variables that can influence users' confidence, including trust, contentment, loyalty, and word-of-mouth. In addition, focus groups and interviews are examples of qualitative methodologies that may be used to learn more about users' perspectives and experiences with information security and confidence.

6. References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.
- Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2016). Consumer adoption of mobile banking in Jordan: examining the role of usefulness, ease of use, perceived risk and self-efficacy. Journal of Enterprise Information Management, 29(1), 118-139.
- Alawneh, A., Al-Refai, M., & Batiha, K. (2013). Measuring user satisfaction from e-banking services: a case study. International Journal of Information Technology and Management, 12(3), 237-252.
- Almaiah MA, Al-Rahmi A, Alturise F, Hassan L, Lutfi A, Alrawad M, Alkhalaf S, Al-Rahmi WM, Al-sharaieh S, Aldhyani THH. (2022). Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in Saudi Arabia. Electronics. 11(23):3926.
- Alshammari, M., & Alhussain, H. (2021). Investigating IT Governance Practice and Its Application, Benefits, and Administrative Implications in the Private Banking Sector in Saudi Arabia. International Business Research, 14(9), 1-12.
- Alzahrani, A., & Alharbi, A. (2023). Exploring Customer Awareness towards Their Cyber Security in the Banking Sector in Saudi Arabia. Human Behavior and Emerging Technologies, 5(1), 1-10.
- Alzamil, Zakarya. (2018). Information Security Practice in Saudi Arabia: Case Study on Saudi Organizations. Information and Computer Security. 26. 00-00. 10.1108/ICS-01-2018-0006.
- BCG. (2023). https://www.bcg.com/publications/2023/performance-of-banking-sector-in-saudi-arabia

- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2012). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 31(3), 418-431.
- Cheng, X., Fu, S., & de Vreede, G. J. (2021). Users' confidence in social media security and privacy: A study of perceived usefulness, ease of use, security, privacy, and quality. Computers in Human Behavior, 114, 106557.
- Cram, W.A., Proudfoot, J.G. & D'Arcy, J. Organizational information security policies: a review and research framework. Eur J Inf Syst 26, 605–641 (2017).
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.
- Elamin, Bushra. (2016). The Impact Of Information Security Management For E- Banks Performance In Kingdom Of Sudi Arabia. 10.5281/zenodo.166827.
- Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. CSO Online: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html.
- Furnell, S. (2005). Why users cannot use security. Computers & Security, 24(4), 274-279.
- Gilman Ranogajec, A., & Badurina, A. (2021). The effect of framing on social media users' privacy calculus. Computers in Human Behavior, 114, 106568.
- Gilman Ranogajec, M., & Badurina, B. (2021). Measuring users' confidence in social media security and privacy. Education for Information, 37(4), 427-442
- Grasshoff, G., Bohmayr, W., Papritz, M., Leiendecker, J., Dombard, F., & Bizimis, I. (2018). Banking's Cybersecurity Blind Spot—and How to Fix It. Boston Consulting Group.
- Hamakhan, Y. T. M. (2020). The effect of individual factors on user behaviour and the moderating role of trust: an empirical investigation of consumers' acceptance of electronic banking in the Kurdistan Region of Iraq. Financial Innovation, 6(1), 43
- Humaidi N, Balakrishnan V. Indirect effect of management support on users' compliance behaviour towards information security policies. Health Information Management Journal. 2018;47(1):17-27.
- ISO/IEC 27004:2016 - Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation: https://www.iso.org/news/2016/12/Ref2151.html.
- ISO/IEC 27018:2019 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: https://www.iso.org/standard/76559.html.
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.
- Kizza, J. M. (2019). Guide to computer network security (5th ed.). Springer.
- Kraus, L., Wechsung, I., & Möller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. Journal of Information Security and Applications, 34, 34-45.
- Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. Electronic Commerce Research and Applications, 8(3), 130-141.
- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems, 54(1), 471-481.
- Liao, Z., & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: an empirical study. Information & Management, 39(4), 283-295.

- M. Dhingra and R. K. Mudgal. (2019)."Applications of Perceived Usefulness and Perceived Ease of Use: A Review," 8th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2019, pp. 293-298,
- Pfleeger, C. P., & Pfleeger, S. L. (2015). Analyzing computer security: a threat/vulnerability/countermeasure approach. Pearson Education.
- Sabau, C. (2022). 5 Ways in Which Banks Secure Their Data. Endpoint Protector.
- SABB awarded Best Private Bank in Saudi Arabia for 2023.
- Sharma, K., Zhan, X., Nah, F. F.-H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. Organizational Cybersecurity Journal: Practice, Process and People, 1(1), 69-91
- Sharma, S., Kaur, G., & Singh, A. (2021). Digital nudging for cybersecurity: A systematic literature review. Computers & Security, 105, 102212.
- Sharma, S., Kaur, R., & Singh, M. (2021). Digital nudging for information security behavior: A framing and priming approach. Computers & Security, 103, 102181.
- Stallings, W., & Brown, L. (2018). Computer security: principles and practice (4th ed.). Pearson Education.
- Tahani Abdullah Abdurhman Alhumud, Abdulfattah Omar & Waheed M.A. Altohami (2023) An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach, Cogent Education, 10:2.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS quarterly, 425-478.
- Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.
- Zhang, J., Luximon, Y., & Song, Y. (2019). The Role of Consumers’ Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness in Continuous Use of Mobile Payment Services. Sustainability, 11(23), 6843.