Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

CYBER-SECURITY EFFICACY AND FINANCIAL PERFORMANCE OF FINTECH COMPANIES IN NIGERIA

IMOH, JULIA IFEYINWA
Department of Accountancy, Faculty of Business Administration, University of Nigeria, Enugu Campus, Enugu State, Nigeria.

EMENGINI, EMEKA STEVE *
Department of Accountancy, Faculty of Business Administration, University of Nigeria, Enugu Campus, Enugu State, Nigeria. (* Corresponding Author)

IMOH, OSITA JUSTIN
Department of Economics, Faculty of Social and Management Science, Kaduna State University, Nigeria.

Abstract

Against the backdrop of producing empirical evidence that supports a rewarding return on investments in cyber security efficacy, this study investigated the degree of influence cyber security efficacy exerts on financial performance using primary source for data collection. Fintech companies in Nigeria were taken as the study population. Cyber security efficacy was operationalized in terms of access restriction capacity (ARC), attack resistance capacity (ATC) and self-preservation capacity (SPC), while return on asset (ROA) was used as proxies of financial performance. Top management support was utilized as the contextual factor in relating cyber security efficacy to financial performance. Multiple linear regression technique was used as the principal too of statistical analysis while Pearson's Product Moment Correlation was used in supporting role. On the final analysis, it was found that analysis produced evidence that access restrictions capacity of digital products of Fintech companies in Nigeria significantly exerts positive influence on their return on assets. Also, analysis showed that attack resistance capacity of digital products of Fintech companies in Nigeria exerts significant positive influence on their return on assets. It was also found that self-preservation capacity of digital products of Fintech companies in Nigeria exerts significant positive influence on their return on assets. Lastly, it was found that top management support level at Fintech companies in Nigeria significantly moderates the degree of relationship between their cyber security efficacy and return on assets. It is therefore concluded that if the full potentials of online payments, e-commerce and other digital product markets have to be realised, then it is incumbent on Fintech companies to make significant amount of investments that have direct bearing on the efficacy of cyber security. Based on the results and conclusions, we recommend that Fintech companies should improve on the use of multiple layer system of user ID authentication that includes bio-metric means, among others.

Keywords: Cybersecurity Efficacy, Financial Performance, Fintech Companies, Nigeria.

1. INTRODUCTION

It is no gain saying that; criminality has taken a new dimension different from what was obtainable previously in which physical assaults was the order of the day (Ojeka, Ben-Caleb & Ekpe, 2017). Gone are the days when incidences of clandestine scheme of inventory pilferages, or real profit erosion due to stealing in obscurity, or other forms of assets misappropriation were the preferred style of fraud in nowadays organisations. In contemporary time, this style has become old fashion. Corporate fraud these days are increasingly becoming digital. Also from external intrusion perspective, broad day robbery

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

and invasion of banking premises are increasingly becoming rare. It is against this backdrop that Rajendra (2018) declared that these days, "*lawbreakers don't ransack institutions with firearm, or assault the employees with weapons yet they assault with more modern weapons like keyboard, mouse, and software program and network algorithms*". Arguably, no business is more vulnerable to this growing sophistry of criminality than Fintech companies and their customers, especially because of the frequency of their online real time presence and propensity to propagate the gospel of cashless banking policy.

Cyber security refers to a data framework utilized in opposing dangers from the internet, which may bargain the accessibility, honesty, or privacy of information (Njeru & Gaitho, 2019). Digital protection (Cyber security) is frequently utilized as a similar to term for data security. Cyber security is not really just the insurance of the actual internet, yet additionally the security of the individuals who work in the internet and any of their resources that can be reached by means of the internet (Albrechtsen & Hovden, 2010). Cyber security contains advancements, cycles and controls that are intended to secure frameworks, organizations and information from digital assaults. Powerful network safety (effective cyber security) lessens the danger of digital assaults (cyber-attack resistance) and secures social orders, associations and people from the unapproved abuse of frameworks (i.e. access restriction), organizations and advances. According to Gordon and Loeb (2006), the destinations of digital protection can be separated into three general classes. In the first place, network safety secures the classification of private data; second, it guarantees that approved clients can get to data on an opportune premise and third, digital protection ensures the exactness, unwavering quality and legitimacy of data. The imperativeness of cyber security, from organisational context, is to boost customer's confidence.

It is common knowledge that the success of any Fintech company is profoundly rooted in the confidence level of its target clients on the security and safety assurance offerings of its product/service regarding their privacy. Accordingly, anxiety about cyber security is expected to be peculiar to Fintech companies, especially. Thinking in similar direction, Yayla and Hu (2011), as earlier observed by Cavusoglu and Zhang (2008), that customers' perception of organizations' security activities significantly affects their standing and market esteem. Thus the submission by Yayla and Hu (2011) has far-reaching implication for the nexus between cyber security efficacy and performance of businesses whose operations depend largely on cyber space. A reasonable degree of business activities of Fintech companies are conducted via the cyber space. Like e-commerce, digital banking has exploded globally since the pandemic; so much so that experts project digital banking users to reach over 3.6 billion globally by 2024, (The Guardian, 2023). According to reports, over 200 Fintech firms in Nigeria provide online access to mobile payments, digital banking, and commercial and personal finance activities, (The Guardian, 2023). For a business that depends so remotely on cyber space for its going-concern, customers' worries about cyber security is likely to eat deep into their profitability. Hence, just as worry concerning cyber security negatively associates

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

with their profitability, it is a general expectation that measures taken to boost cyber security should associate positively with their financial performance. In other words, efficacy in the implementation of cyber security strategies may affect the performance of Fintech companies.

Linking cyber security efficacy to financial performance has become necessary for the Fintech industry due to popular thinking that investments in cyber security enhancement undermine profitability. In recent time, several studies (Klinle & Renn, 2011; Bromiley, McShane, Nair & Rustambekov, 2014; Pagach & Warr, 2011) have suggested that firms in the Nigerian Fintech industry face a growing number of new and interrelated risks compared to their peers in other sectors. KPMG (2016) reported that financial institutions in Nigeria lose averagely about 10 billion naira yearly due to avoidable and unsystematic risk, posed majorly by cyber insecurity. They advocated for a more integrated and holistic approach to tackling risk issues in the Nigerian financial industry. The prospect of dealing with rising cost profile that will follow from such project might pose a source of discouragement against investments in cyber security. It is therefore an academic necessity to produce empirical evidence that confirms or debunks the association of profit erosion with investment in cyber security once and for all.

Although there was stiff resistance against it, with the launch of the Naira Redesign Policy by the Central Bank of Nigeria which was implemented on Wednesday, November 23rd 2023, it is almost certain that volume of digital banking will be on the rise. The initial resistance against the policy is a confirmation of customers' apprehension over the state of cyber security in Nigeria. This worry is being substantiated in terms of poor network, failed transactions, and cases of unauthorised debits in accounts of customers often experienced during the use of online platforms across the country. Considering the role of the financial technology firms in the Nigerian economy, there is no doubt that the impact of customers' loss of confidence in online payment platforms will be enormous. To build confidence in customers, Fintech companies, banks and other financial companes that depend on cyber space to service their customers are required to make strategic investments that are aimed at enhancing the efficacy of cyber security. In recognition of this requirement, the Nigerian government through enactment in 2015 ordered the Cybercrime Act. The Act gives a viable, bound together and far-reaching legitimate, administrative and institutional structure for the disallowance, counteraction, location, arraignment and discipline of cybercrimes in Nigeria (Njeru, & Gaitho, 2019; Nweke, 2017). It likewise guarantees the assurance of basic public data framework, and advances network safety and the security of PC frameworks and organizations, electronic correspondences, information and PC programs, protected innovation and security rights. The government alone is not reassuring enough. The private sector is also required to act. Thus there is no better time for Fintech companies to build customers' confidence in the capacity of Nigeria's online payment platforms than now. It is therefore imperative to encourage Fintech companies and others whose operations depend largely on the use of cyber space. One way this can be done is to allay concerns of Fintech companies that investments in cyber security might undermine their financial performance.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

Despite the fact that a number of literary works has been done partially on the subject, the current work is still necessary for a number of reasons. Unlike the study by Khalil, Manzoor, Tahir, Khan and Jamal (2021) which sought to analyse the association among cyber security costs, such as prevention and detection costs (PDC), response costs (RC), development costs (DC), and indirect costs (IC), on the e-banking product innovation performance (PIP) and financial performance (FP), the current study seeks to investigate if cyber security efficacy has a rewarding relationship with financial performance. The main difference being that the former is focused on cost while the latter is focused on efficacy. Cost represents investment, no doubt, but spending a certain amount on cyber security does not necessarily translate to its enhanced efficacy. The present study on the other hand seeks to investigate the impact of cyber security efficacy on financial performance. Besides, the former is a study on foreign bank which shares very little or no affinity with the latter, thus creating a gap with regards to the study population. Perhaps the only Nigerian study that comes close to sharing similarity with the current study is one by Akintoye, Ogunode, Ajayi and Joshua (2022) which sought to examine the impact of cyber security in driving the financial innovation of Deposit Money Banks in Nigeria. However, this study also falls short of meeting the objective of the current study stated earlier. Though the two studies share similar study population, they differ in the core objective. The absence of prior study that should have served as yardstick for evaluating how cyber security efficacy rewardingly relates with financial performance thus creates a gap in literature which the current study seeks to fill. Accordingly, the study seeks to evaluate the relationship between efficacy of cyber-security efficacy and financial performance of Fintech companies in Nigeria. The specific objectives are to determine the extent to which access restrictions capacity of digital products can influence return on assets of Fintech companies in Nigeria; examine the degree to which attack resistance capacity of digital products can influence return on assets of Fintech companies in Nigeria; ascertain the magnitude of influence which self-preservation capacity of digital products can exert on the return on assets of Fintech companies in Nigeria; and ascertain the degree to which top management support level can moderate how cyber security efficacy affects performance of Fintech companies in Nigeria.

The rest of the paper proceeds as follows: section-2 presents literature review, section-3 on the other hand presents methodology; section-4 presents results of the study and finally section-5 provides the study's conclusion.

2. LITERATURE REVIEW

2.1 Theoretical Framework

The link between cyber security efficacy and financial performance is anchored on the resource-based view (RBV) theory which is a managerial framework used to determine the strategic resources a firm can exploit to achieve sustainable competitive advantage. It focuses managerial attention on the firm's internal resources in an effort to identify those assets, capabilities and competencies with the potential to deliver superior competitive

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

advantages. The resource-based view offers strategists a means of evaluating potential factors that can be deployed to confer a competitive edge. A key insight arising from the resource-based view is that not all resources are of equal importance, nor do they possess the potential to become a source of sustainable competitive advantage (Fahy & Smithee, 1999). The sustainability of any competitive advantage depends on the extent to which resources can be imitated or substituted, (Lowson, 2003). In the resource-based view, strategists select the strategy or competitive position that best exploits the internal resources and capabilities relative to external opportunities. Given that strategic resources represent a complex network of inter-related assets and capabilities, organisations can adopt many possible competitive positions. Thus for Fintech companies, cyber space security efficacy can represent strong unique resource. A unique resource is a resource that competitors would have difficulty in acquiring or imitating; therefore they are a source of competitive advantage. Fintech firms that have more unique resources such as cyber-space security efficacy are most likely to attract more customers, hence are more likely to attain higher financial performance. Thus in theory, a positive relationship should exist between cyber security efficiacy and financial performance, since customers seek for digital platforms that would guarantee the security and safety of their privacy. In otherwords all things being equal, a firm with poor cyber security efficacy is only likely to be compensated with poor demand for its services/products just as one with high security efficacy is likely to be rewarded with high demand for its services/products. While the contextual factor in this postulation can range from a wide variaeties firm-specific attributes, we opt to use existing tone-at-the-top. Hence the study is basically comprised of three main variables (also known as constructs), which are Cyber Security Efficacy (CSE), Financial Performance (FP) and Tone-at-the-Top.

Cyber Security Efficacy is the criterion variable while Financial Performance is the response variable. Tone-at-the-Top is a moderator (i.e. a variable that is expected to have relationship with both the response and dependent variables) is expected to moderate the relationship between the two principal variables. In the context of *access restriction capacity* (ARC), *attack resistance capacity* (ATC) and *self-preservation capacity* (SPC) as the dimensions of cyber security efficacy, the RBV theory predicts a positive relationship between each of the dimensions of cyber security efficacy and financial performance (ROA as proxt). Figure-1 represents the overall structure of the study and the *apriori* expectation according to the RBV theory.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

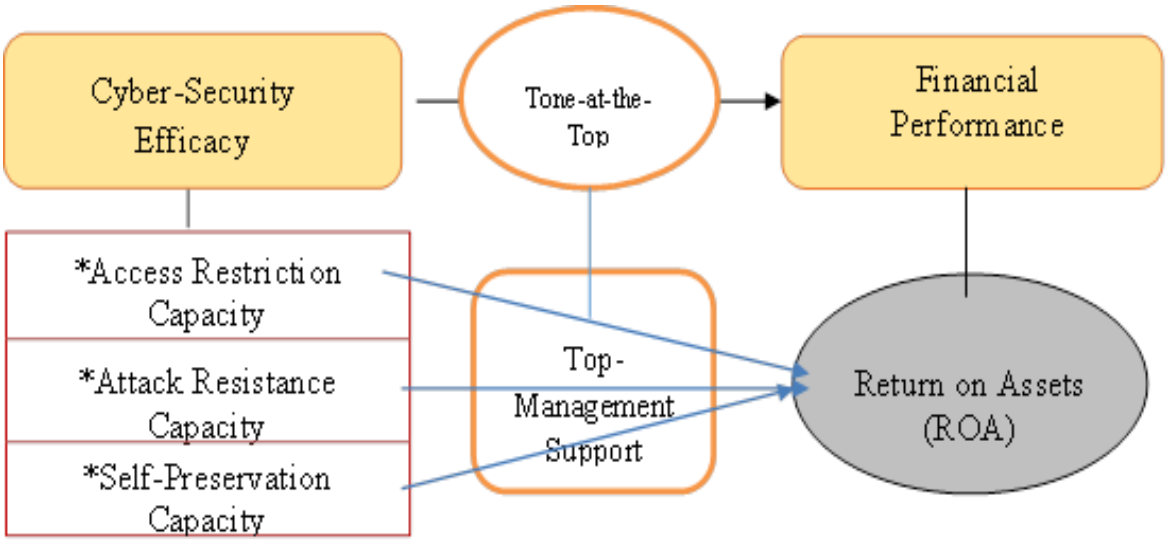

Figure 1: Conceptual Framework of Cyber-Security Efficacy and Financial Performance

2.2 Hypothesis Development: Cyber Security Efficacy and Financial Performance

The '*safety and security of privacy concern*' hypothesis is the umblical cord that connects cyber security efficacy to financial performance. Confidence level in safety and security of individual privacy is directly proportional to individual's demand for cyber products and services (Ali, Ali, Surendran &Thomas, 2016). Hacking and abuse of online-based payment platforms are only possible if and when a perpetrator gains unauthorised accesses to the digital space. With the prevalence of an effective access restriction capacity, and/or effective intrusion detection mechanism such that unauthorised access is restricted, cyber crime rate is likely to be reduced significantly. Reduction in rate of security breach occurrence also reduces the likelihood of financial loss exposure due to access compromise. With a noticeable reduction in rate of security breach occurrence, online customers' confidence in the safety and security of their privacy is expected to rise (Ali, *et al*, 2016), hence we expect to see a positive relationship between access restriction capacity and financial performance (Tumba, Onodugo, Akpan & Babarinde, 2022).

Empirical literature is replete with findings that support our postulation. For instance, Khalil, Manzoor, Tahir, Khan, & Jamal, (2021) examined the impact of Cyber Security Cost on the financial performance of E-Banking in Pakistan. It was found that detection cost, response cost and development cost have a statistically significant effect on FP. Since cyber security cost is a financial consequence of cyber security decision aimed at enhancing its efficacy, it logically consistent to expect a positive relationship between cyber security efficacy and financial performance. Similarly in Nigeria, Akintoye, Ogunode, Ajayi, & Joshua, (2022) also investigated the relationship between cyber

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

security and financial innovation of selected Deposit Money Banks in Nigeria. The study found that cyber security proxied by risk management and bank monitoring had a statistically and positively significant impact on financial innovation of DMB in Nigeria. This alludes to the fact that cyber security is a major determinant of the confidence level of online customers in the safety and security of their privacy. It has been empirically confirmed that almost 70% of online customers have limited or no awareness about the threats available to individual and banking industry; more than 60% users are unable to identify and handle the existing information security threats; about 55% users do not take any extra care when dealing with online banking services, (Ali, *et al*. 2016). The greater the gap in knowledge is, the higher the intensity of the concern is. In the light of the foregoing therefore, the following null hypotheses are suggested for testing:

H_{01}: Access restrictions capacity of digital products of Fintech companies in Nigeria does not exert significant influence on their return on assets.

H_{02}: Attack resistance capacity of digital products of Fintech companies in Nigeria does not exert significant influence on their return on assets.

H_{03}: Self-preservation capacity of digital products of Fintech companies in Nigeria does not exert significant influence on their return on assets.

H_{04}: Top management support level at Fintech companies in Nigeria does not significantly moderates the degree of relationship between their cyber security efficacy and return on assets.

3. METHODOLOGY

The paper survey method is deemed most appropriate for primary data collection due to its relative ease to administer, cost-effectiveness and general adaptability with respondents of varying demographics (Ibekwe, et al., 2020). The study population is Fintech companies in Nigeria. Accordingly, the population of study comprises of all the 236 members of companies listed by Adeyemi, Ehiwari and Dairo (2022) in the web page: www.linkedin.com/pulse/2022-nigeria-fintech-map-year-review-segun-adeyemi. The 2022 list features 232 companies under 14 categories. Hence the population is finite, and considerably large. In line with Taro Yemen's formula, since the population is finite (232) and fairly large, a sample size of 147 (one hundred and forty-seven) is determined to be appropriate. This is further apportioned among fourteen categories of Fintech companies in Nigeria.

Both interviews and paper survey techniques were applied. Expert opinions from IT professionals were sought on how to measure cyber security (in terms of the three dimensions). The questionnaire was used to obtain and gather information as regards to 'Cyber security efficacy and financial performance using the 5- point Likert scale. The model used to test the study's hypotheses is stated as follows:

$$PERF = f(ARC, ATC, SPC) \quad \text{Eqn. (1)}$$

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

where *PERF* is financial performance. Since PERF is measured in terms of returns on asset (ROA), the model is specified in econometric form as follows:

$ROA_i = b_0 + b_1 ARC_i + b_2 ATC_i + b_3 SPC_i + E$ Eqn. (2)

Where E is error terms; b_0 is parameters representing the intercepts of the regression equations; b_1 is ROA response coefficients of access restriction capacity of digital products; b_2 is ROA response coefficients of attack resistance capacity; and b_3 is ROA response coefficients of self-preservation capacity of digital products. In line with the theoretical underpinnings of the study, our *a priori* expectation with respect to the response coefficients are b_1, b_2, and $b_3 > 0$.

4. RESULT

4.2.1 Access Restriction Capacity

Results from the survey are presented in table-2.

Table 2: Access Restriction Capacity of Digital Products

S/N	Items	Mean Score	Std Dev	Verdict
1	Strictness of minimum character length enforcement as password policy	3.99	1.343	Agree
2	Strictness of multiple layer system enforcement as password policy	3.44	1.271	Undecided
3	Enforcement of the use of bio-metric means of authentication as password policy	3.69	1.184	Agree
4	Rarity of password compromise being above maximum expected frequency	3.63	1.160	Agree
5	Frequency of password policy review to meet up international best practices	3.72	1.241	Agree
	Aggregate	**3.70**	**1.249**	**Agree**

Source: Field Survey, 2023

According to table-2, respondents' collective opinion on the average is 3.7 on the 5-point Likert scale. This indicates an affirmation of high prevalence of access restriction capacity of digital products which are offered to their customers by Fintech companies in Nigeria. As suggested by the result from table-2 (item 1), the high prevalence of digital product access restriction is mostly attributed to firms' password policy on strictness of minimum character length enforcement. Item-1 is the highest while the least prevalent factor is firms' password policy on multiple layers system enforcement. The overall standard deviation suggests a high variability of access restriction capacity among the respondents, a factor which can be attributed to divergence in organisational and operational structures.

In order to ascertain the uni-dimensionality of the five (5) items of access restriction capacity, and also to convert the ordinal scale result to interval scale, a factor analysis was carried out.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

To test for the suitability of carrying out a factor analysis, a KMO-Bartlett test was carried out. The results strongly confirms the suitability of carrying out factor analysis since the p-value is less than 0.05 and the high values of the KMO statistic (0.900) which generally indicate that a factor analysis is useful with the data.

According to the result on the factor analysis, there is only one component that was extracted which explains 85.2 per cent of the total variance, with an Eigen value of 4.260. This means more than four out of the five items used to measure access restriction capacity were able to go in the same direction in the measurement of the variable.

The Cronbach alpha of 0.956 for all the five items indicates an acceptable level of internal reliability and consistency. Since the foregoing statistics indicate high degree of reliability and validity of measurement, the estimated principal component can suitably serve as measured observation of access restriction capacity.

4.2.2 Attack Resistance Capacity

Results from the survey are presented in table-3.

Table 3: Attack Resistance Capacity of Digital Products

S/N	Items	Mean Score	Std Dev	Verdict
1	Producers' prioritization of intrusion detection capabilities of digital products	3.75	1.323	Agree
2	Producers' implementation of policy on Intrusion Detection Sensors (IDS) installation in digital products	3.67	1.175	Agree
3	Acceptability of producers' Intrusion Detection and Prevention standard of digital products	3.84	1.165	Agree
4	False alarm rate of intrusion detection system of digital products being less than the minimum expected frequency	3.66	1.041	Agree
5	Rarity of viral attacks on digital products being greater than minimum expected frequency	3.78	1.375	Agree
	Aggregate	**3.74**	**1.220**	**Agree**

Source: Field Survey, 2023

According to table-3, respondents' collective opinion on the average is 3.74 on the 5-point Likert scale. This indicates an affirmation of high prevalence of attack resistance capacity of digital products which are offered to their customers by Fintech companies in Nigeria. As suggested by the result from table-3 (item 3), "*acceptability of producers' IDP standard of digital products*" is mostly attributed to attack resistance capacity of Fintech's digital products. On the other hand, item-4 ("*false alarm rate of intrusion detection system of digital products being less than the minimum expected frequency"*) is the least prevalent factor. The overall standard deviation suggests a high degree of randomness in the measurement of attack resistance capacity based on the respondents' collective opinions.

Similarly, a factor analysis was conducted in order to determine the weight of the underlining factor in based on the five manifest constructs used, and also to convert the ordinal scale result to interval scale so as to permit compatibility with regression analysis.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

As a proof of sampling adequacy and satisfaction in meeting requirements for factor analysis, KMO and Bartlett's test was conducted.

The results resoundingly confirm the suitability of carrying out factor analysis at 1% significance level. Again, the high values of the KMO statistic (0.871) which generally indicate that a factor analysis is useful with the data, further gives impetus for using principal component analysis with negligible risk of error.

Therefore, according to the result on the factor analysis (see appendix), there is only one component that was extracted which explains 87.355 per cent of the total variance, with an Eigen value of 4.368. This means more than four out of the five items used to measure attack resistance capacity were able to go in the same direction in the measurement of the variable.

As a measure of internal consistency and reliability, the Cronbach alpha was used. A score of 0.956 for all the five items shows that there is high degree of reliability. Thus the foregoing univariate analyses support the position that the estimated underlying component can befittingly serve as measured observation of attack resistance capacity.

4.2.3 Self-Preservation Capacity

Results from the survey are as stated in table-4. In line with the adopted cut-off range, table-4 appears to indicate that the overall respondents' collective opinion on the prevalence of self-preservation capacity of digital products sold by Fintech companies is neither confirmed nor refuted.

Table 4: Self-Preservation Capacity of Digital Products

S/N	Items	Mean Score	Std Dev	Verdict
1	Producers' placement of premium on product capability to ensures its continuous operation	3.72	1.265	Agree
2	Inbuilt capability to identify and report on compatibility breach within its operating environment	3.58	1.210	Agree
3	Capability of to initiate auto-debugging mechanism	3.84	1.270	Agree
4	Capability to automatically shut out users the moment the number of allowed authentication test trials elapses.	3.46	1.148	Undecided
5	Inbuilt capability to automatically upgrade to newer versions as soon as they become available	2.78	1.036	Undecided
	Aggregate	**3.48**	**1.241**	**Undecided**

Source: Field Survey, 2023

The overall average score is 3.48 on the 5-point Likert scale. As suggested by the result from table-4, item 3 (*"Capability of to initiate auto-debugging mechanism"*), is the highest contributor to the prevalence of self-preservation capacity of digital products, while item 5 ("*Inbuilt capability to automatically upgrade to newer versions as soon as they become available*") is the least contributor to the prevalence of self-preservation capacity of digital products of Fintech companies in Nigeria. The overall standard deviation suggests that

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

there is high degree of deviation in using the overall average to represent the collective opinion on the extent of prevalence of self-preservation capacity in the industry.

Again, since a number of constructs are being used to determine self-preservation capacity as a variable, it might help to gain more analytical insight if factor analysis is conducted. This is expected to add a number of benefits to the study. Firstly, it enables the determination of the degree to which all five constructs contribute in measuring self-preservation capacity as the underlying factor. Secondly, it enables the conversion of ordinal scale results obtained to interval scales so that regression analysis can be done with the results.

To test for the suitability of carrying out a factor analysis, a KMO-Bartlett test was similarly carried out. The results strongly confirms the suitability of carrying out factor analysis since the p-value is less than 0.05 and the high values of the KMO statistic (0.835) which generally indicate that a factor analysis is useful with the data.

According to the result on the factor analysis (see appendix), there is only one component that was extracted which explains 75.119 per cent of the total variance, with an Eigen value of 3.756. This means more than three out of the five items used to measure self-preservation capacity were able to go in the same direction in the measurement of the variable. This is above the rule-of-thumb criteria of a third (i.e. 33.333 percent) of the items.

The Cronbach alpha of 0.914 for all the five items indicates an acceptable level of internal reliability and consistency. Hence, since the foregoing statistics support high degree of reliability and validity of measurement, the estimated underling factor can suitably serve as measured observation of self-preservation capacity.

4.2.4 Top Management Support

Results from the survey are presented in table-5. As presented in table-5, respondents' collective opinion on the average is 3.65 on the 5-point Likert scale. This indicates a confirmation that high prevalence of TMS for cyber security policy was observed among Fintech companies in Nigeria during the period of the study. According to table-5, items 3 and 4 (i.e. "*top Management's awareness of cyber security benefits*" and "*adequacy of resource provision by top management for implementation of cyber security policy*") respectively are the two aspects of TMS that contributed mostly to the effectiveness of TMS for cyber security policy of Fintechs in Nigeria. On the other hand, item-1 (i.e. "*top Management's provision of administrative assistance in cyber security implementation"*) is the least prevalent factor. The overall standard deviation indicates a high degree of deviation in the measurement of TMS based on the respondents' collective opinions.

In the same way, a factor analysis was conducted in order to establish the weight of the underlining factor based on the five manifest constructs used, and also to convert the ordinal scale result to interval scale so as to permit compatibility with regression analysis. To ensure proof of sampling adequacy and satisfaction in meeting requirements for factor analysis, we similarly conducted KMO and Bartlett's test. The results (both KMO stat and

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

Bartlett's test) unquestionably concur that factor analysis is ideal for the set of data at 1% significance level, hence the impetus to proceed to carrying out a principal component analysis.

Table 5: Top Management Support for Cyber Security Policy in Fintechs

S/N	Items	Mean Score	Std Dev	Verdict
1	Top Management's provision of administrative assistance in cyber security implementation	3.56	1.160	Agree
2	Top management enforces cyber-security policy compliance along the product conception up to production value-chain	3.66	1.320	Agree
3	Top Management's awareness of cyber security benefits	3.74	1.398	Agree
4	Adequacy of resource provision by top management for implementation of cyber security policy	3.71	1.256	Agree
5	Top Management's commitment to ensuring firm's achievement of competitive advantage through mitigation of cyber-security risk exposure of its products	3.57	1.172	Agree
	Aggregate	**3.65**	**1.262**	**Agree**

Source: Field Survey, 2023

According to the result, there is only one component that was extracted which explains 86.534 per cent of the total variance, with an Eigen value of 4.327. The implication of this result is that, almost all five items used to measure top management support were able to go in the same direction in the measurement of the variable, which is an indication of high content construct validity.

Apart from validity, measures were equally taken to ascertain if the measurement instrument attained the minimum reliability and consistency threshold, using Cronbach alpha as the yardstick. As also included in the appendix, a score of 0.960 for all the five items shows that the measurement instrument exhibited a high degree of consistency and reliability. Thus the foregoing univariate analyses support the position that the estimated underlying component can befittingly serve as measured observation of top management support.

4.2.6 Return on Asset

Results from the survey are as stated in table-6. In line with the adopted cut-off range, it is reported in table-6 that the overall respondents' collective opinion on the prevalence of return on asset of Fintech companies is affirmed. The overall average score is 3.63 on the 5-point Likert scale with a standard deviation of 1.280. According to table-6, item 3 (*"Two consecutive years of increase in profit per naira asset value"*), is the highest contributor to the prevalence of the attributes of return on asset, while item 1 ("*Consecutive two years improvements in turnover rate*") is the least contributor to the prevalence of the attributes of return on asset of Fintech companies in Nigeria. The overall standard deviation suggests that there is high degree of randomness in using the overall average to represent the collective opinion on the extent of prevalence of return on asset's

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

attributes in the industry. This randomness is attributable to heterogeneity factors in the circumstances of the firms operating in the industry.

Table 6: Return on Asset of Fintech Companies in Nigeria

S/N	Items	Mean Score	Std Dev	Verdict
1	Consecutive two years improvements in turnover rate	3.54	1.122	Agree
2	Two consecutive years of improvement in assets utilization efficiency	3.63	1.302	Agree
3	Two consecutive years of increase in profit per naira asset value	3.72	1.401	Agree
4	Two consecutive years of increase in productivity relative to the firms' assets portfolio	3.64	1.294	Agree
	Aggregate	**3.63**	**1.280**	**Agree**

Source: Field Survey, 2023

The fact that fewer numbers of constructs are being used to determine return on asset as a variable makes it more imperative to test if factor analysis is applicable as previously conducted with other variables. To test for the applicability of carrying out a factor analysis, a KMO-Bartlett test was executed. The results strongly confirms the suitability of carrying out factor analysis since the p-value is less than 0.05 and the high values of the KMO statistic (0.861) which generally indicate that a factor analysis is beneficial with the data.

According to the result on the factor analysis (see appendix), there is only one component that was extracted which explains 87.123 per cent of the total variance, with an Eigen value of 3.485. This means more than three out of the four items used to measure the return on asset of Fintech companies in Nigeria were able to go in the same direction in the measurement of the variable. With an Eigen value constituting 87.123 per cent, it is safe to report that the measured return on asset achieved that much construct validity.

Also, the internal reliability and consistence of the measurement instrument as measured by Cronbach alpha had a score of 0.949 for all the four items used. This is an indication of an acceptable level of internal reliability and consistency; hence, the estimated underling factor can suitably serve as measured observation of the return on asset of Fintech companies in Nigeria. In summary of the descriptive analysis of the variables, table-7 reports the basic descriptive statistics of the variables derived which are included in the appendix.

Table 7: Descriptive Statistics

	N	Minimum	Maximum	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
ARC	134	-2.012	1.147	-.600	.209	-1.063	.416
ATC	134	-1.744	1.120	-.316	.209	-1.467	.416
SPC	134	-2.052	1.269	-.602	.209	-1.034	.416
TMS	134	-1.732	1.158	-.589	.209	-1.328	.416
ROA	134	-1.773	1.156	-.535	.209	-1.363	.416

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

Valid N (listwise)	134						

Source: SPSS, version 25

4.3 Inferential Analysis of Research Hypotheses

The evaluation of these hypotheses essentially requires the estimation of the parameters of the following analytical equation:

$$ROA_i = b_0 + b_1ARC_i + b_2ATC_i + b_3SPC_i + E \qquad \text{Eqn. (3.3)}$$

With the aid of SPSS (version 25), the results of the estimation, based on the collected data which were subjected to transformation, are presented in table-8 as follows:

Table 8a: Coefficients of ROA Equation

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.130E-17	.048		.000	1.000		
	ARC	.419	.103	.419	4.062	.000	.219	4.573
	ATC	.170	.069	.170	2.452	.016	.486	2.058
	SPC	.309	.101	.309	3.052	.003	.227	4.406

In line with the produced results according to table-8a, the ROA response coefficients of ARC, ATC and SPC are respectively 0.419, 0.170 and 0.309, all of which have positive sign. While ARC and SPC are significant at 1% level that of ATC is at 5% level hence they are all significant.

In regards to the question of whether the model fulfilled the requirements of OLS, the collinearity statistics are respectively below the 10 point rule-of-thumb, hence no need to worry over multicollinearity and its bias-causing effects on the estimated standard errors of the respective coefficients. Also, table4.21b reported Durbin-Watson statistic that signposts a negligible presence of autocorrelation. Concerning the model's goodness-of-fit, the computed coefficient of determination which is adjusted for degree of freedom, indicates a ROA explanatory capacity of all three dimensions of cyber security efficacy jointly. It means that 69.1 per cent of variability in the ROA of Fintech companies in Nigeria can be attributed to the joint variability of all three dimensions of their cyber security efficacy.

Table-8b: Model Summary ROA Equation

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.835[a]	.698	.691	.556306	1.399

Table-8c shows that the ROA equation is properly fitted to the data used at 1% significance level, thus supporting the fact that the estimated coefficients are a true reflection of the structural relationship of the data used. Therefore, the estimated coefficients are respectively the best unbiased estimator of ROA of Fintech companies in Nigeria.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

Table 8c: ANOVA of ROA Equation

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	92.768	3	30.923	99.919	.000[b]
	Residual	40.232	130	.309		
	Total	133.000	133			

Lastly on the robustness of the estimation model, figure-2 presents statistical evidence that the reported probability values of the respective coefficients are free of biases. It is one of the requirements that the distribution of the error term must be normal if the p-value is to be unbias. As a unique characteristic that is perculiar to normality, the mean and the standard deviation are always 0 and 1 respectively. Accordingly in figure-2, the mean (0.000) is approximately zero and the standard deviation (0.989) is approximately 1, hence the proof that the p-values are reliable.

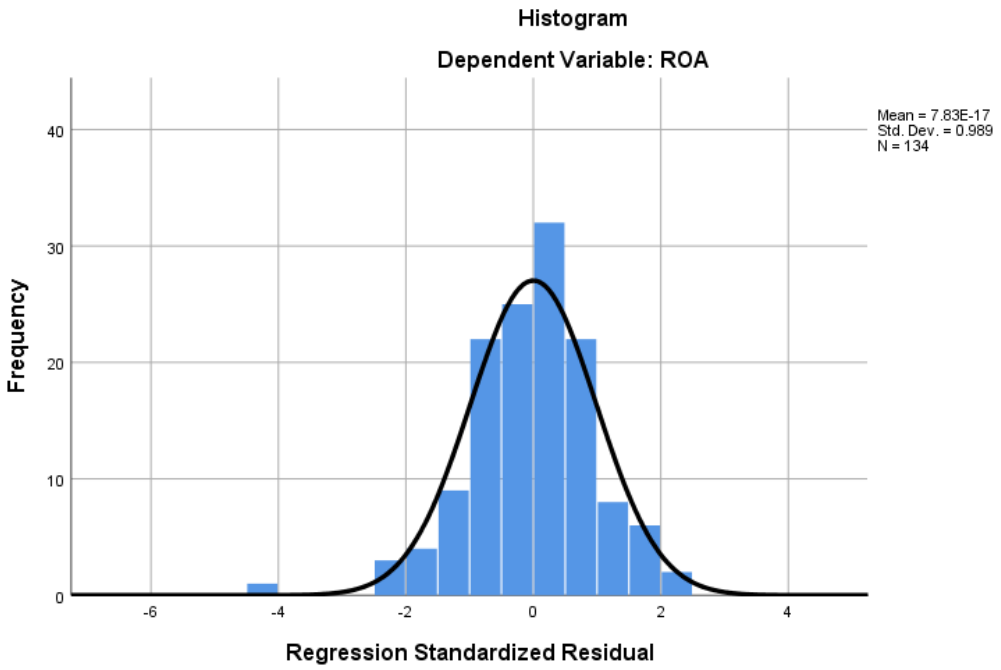

Figure 2: Test of Normality (ROA)

From the foregoing multivariate (multiple linear regressions) analysis therefore, it can be deduced that the ROA response coefficients of ARC, ATC and SPC are significantly different from zero, to the extent that increases in each one of them is likely to give rise to positive response from ROA. However, for the sake of argument that interaction effects among these independent variables might obscure the relationship strength in any of them with ROA, then corroborating evidence might be required. This is why another level of analysis (e.g. bivariate) is necessary.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

As a further support to the results obtained, table-9 presents bivariate (Pearson's product moment correlation coefficients) analysis of ROA against ARC, ATC and SPC respectively:

Table 9: Correlation Matrix of ROA and Independent Variables

		ARC	ATC	SPC	ROA
ROA	Pearson Correlation	.808**	.675**	.791**	1
	Sig. (2-tailed)	0.000	0.000	0.000	
	N	134	134	134	134

As reported in table-9, the Pearson's Product Moment Correlation (PPMC) coefficient between ROA and ARC is 0.808 with a p-value of 0.000. This means increasing values of ARC is strongly associated with increases in ROA to the extent that approximately 65.3 per cent of the changes in the value of Fintech companies' ROA in Nigeria are attributable to changes in ARC of their digital products. Therefore with respect to hypothesis number 1, there are sufficient statistical justifications from both multivariate and bivariate analyses to strongly reject the null hypothesis. Therefore:

H_{01}:*Access restrictions capacity of digital platforms at Fintech companies in Nigeria does not exert significant influence on their return on asset*

Decision: Reject (meaning *access restrictions capacity of digital platforms at Fintech companies in Nigeria exert significant influence on their return on asset*)

Similarly as reported in table-9, the PPMC coefficient between ROA and ATC is 0.675 and its p-value is 0.000. Again, this means that increasing (decreasing) values of attack resistance capacity of Fintech companies in Nigeria associates with their ROA increasingly (decreasingly). With R being 0.675, R^2 is evaluated to be 0.456 (or 45.6 per cent) approximately, implying that ATC is capable of explaining about 45.6 per cent changing values of the ROAs of Fintech companies in Nigeria. Hence regarding hypothesis number 2, again, both multivariate and bivariate analyses have produced enough statistical proofs to serve as basis to reject the null form of the hypothesis. Therefore:

H_{02}: Attack resistance capacity of digital platforms at Fintech companies in Nigeria does not exert significant influence on their return on assets

Decision: Reject (i.e. *attack resistance capacity of digital platforms at Fintech companies in Nigeria significantly affect their ROAs*)

Lastly on hypothesis number 3, on top of the multivariate analysis which has produced adequate pool of empirical facts in support of rejecting the hypothesis, table-9 also reports result on bivariate analysis in the form of PPMC coefficient to support the same decision. According to the result (PPMC = 0.791; p-value = 0.000), increases in self-preserving capacity (SPC) of digital products of Fintech companies in Nigeria are strongly related to changes in their return on asset to the extent that, changing values of SPC can account for 62.6 per cent (i.e. R^2 = 0.626 approx.) of the changing values of the companies' return

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

on asset. Hence, results of both multivariate and bivariate analyses strongly corroborate each other that the hypothesis in its null form should be rejected. Therefore:

H_{03}: Self-preservation capacity of digital platforms at Fintech companies in Nigeria does not significantly affect their net profits

Decision: Reject (i.e. *Self-preservation capacity of digital platforms at Fintech companies in Nigeria significantly affect their return on asset*)

In overall therefore, the results obtained conclusively corroborate those of Khalil et al., (2021) and Akintoye et al, (2022), at least on the premise that costs or managerial actions taken in an effort to enhance cyber security achieve the desired goals.

4.3.4 Evaluation of Hypothesis on Moderating Role of Top Management Support

Hypothesis to be evaluated is restated as follows:

H_{04}: Top management support level at Fintech companies in Nigeria does not significantly moderates the degree of relationship between their cyber security efficacy and return on assets

At the stage of multivariate analysis, to evaluate the moderating impact of top management support (TMS) will require the estimation of the following analytical equation:

$$ROA_i = \beta_0 + \beta_1 ARC_i + \beta_2 ATC_i + \beta_3 SPC_i + \beta_4 TMS_i + \beta_5 ARC*TMT_i + \beta_6 ATC*TMS_i + \beta_7 SPC*TMS_i + e \quad \text{Eqn. (3.5)}$$

Via the use of SPSS, table 10 reports the result as follows:

Table 10: Coefficients of Moderated ROA Equation

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.054	.031		-1.741	.084
	ARC	-.009	.046	-.009	-.193	.848
	ATC	.097	.033	.097	2.961	.004
	SPC	-.023	.036	-.023	-.628	.531
	TMS	.975	.031	.975	31.440	.000
	ARC_TMS	.132	.049	.119	2.704	.008
	ATC_TMS	-.035	.036	-.032	-.970	.334
	SPC_TMS	-.038	.032	-.035	-1.205	.230

Following the results as displayed in table-10, ARC and SPC of the main variables and two interaction terms (i.e. ATC_TMS and SPC_TMS) failed the significance threshold. On the other hand, ATC, TMS and ARC_TMS scaled through the significance test at 1% significance level. While ATC and TMS are positively related to ROA, the interaction term (ARC _TMS) had a negative slope. Besides the fact that the model's explanatory capacity improved from 0.691 to 0.969, and besides its robustness against OLS infractions also recorded improvement (e.g. DW stat changing from 1.399 to 2.100), at least an interaction

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

terms has a significant coefficient. This is an indication that TMS has significant moderating impact on how ROA relates with ARC.

To confirm the moderating impact of TMS on the relationship between ROA and ARC, another round of analysis is required, this time a partial correlation technique. Under this analytical approach, correlation between ROA and each of ARC, ATC and SPC is respectively computed while controlling for TMS. The respective coefficients are then compared against the earlier computed PPMC coefficients that are corresponding. If either the significance status or the direction of relationship did not change, then there is no moderating effect, otherwise moderating effect is confirmed. Table-11 presents the combined results from table-9 and partial correlation results.

According to table-11, PPMC for ARC versus ROA is 0.808 and the p-value is 0.000. By comparison with the partial correlation result for ARC versus ROA in table-11 which is -0.047, it shows that the former is positively correlated and significant at 1% level, while the latter is negatively correlated and insignificant even at 5% level. This means that TMS possesses significant moderating influence in determining the relationship between ROA and ARC.

Table 11: TMS Moderating Impact on ROA and Cyber Security Efficacy

		ARC	ATC	SPC
Partial Corr (Control TMS)	Correlation	-0.047	0.085	-0.072
	Significance (2-tailed)	0.593	0.329	0.408
	Df	131	131	131
ROA	Pearson Correlation	.808**	.675**	.791**
	Sig. (2-tailed)	0	0	0
	N	134	134	134

With respect to ATC versus ROA, PPMC yielded 0.675 while partial correlation result of the same pair yields 0.085. It turns out that both are positively related, but the partial correlation result is insignificant at 5% level. For the fact that there is difference in significance status, it means that TMS is capable of exerting moderating influence in determining the relationship between ROA and ARC. However this contradicts the multivariate analysis result where the fact indicates the TMS does not have significant moderating influence.

Finally, with regards to SPC versus ROA, PPMC produced a positive coefficient (0.791) with a probability value that is approximately zero. However, the same pair after controlling for TMS under partial correlation yields a negative coefficient (-0.072) with a probability value that is greater than 0.05. Thus here, both sign and significance statuses changed, meaning that TMS is a significant moderator in the relationship between ROA and each one of ARC, ATC and SPC. Again, it is important to note that the moderated regression result failed to support TMS as a significant moderator. However, focus of the analysis is to evaluate the proposition on whether TMS can or cannot moderate how ROA

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

relates with cyber security efficacy. To that extent, the foregoing analysis has provided sufficient justification to conclude in the affirmative.

Therefore with respect to hypothesis 4, there is sufficient statistical evidence to support its rejection. Hence:

H_{04}: Top management support level at Fintech companies in Nigeria does not significantly moderates the degree of relationship between their cybersecurity efficacy and return on assets

Decision: Reject Null Hypothesis

5. CONCLUSION AND RECOMMENDATONS

5.1 Conclusion

The current study has produced conlusive fact that cyber security efficacy has a positive relationship with financial performance. This positive relationship proves that investing in the efficacy of cyber security has the potential to reward Fintech companies financially. Thus Fintech companies possess the capability of reversing the eroding confidence levels of their customers due to prevalence of cyber security breaches. If the full potentials of online payments, e-commerce and other digital product markets have to be realised, then it is incumbent on Fintech companies to make significant amount of investments that have direct bearing on the efficacy of cyber security. It is hoped that such efforts will bolster customers' confidence in cyber security and ultimately unleach the full potential of digital product markets in Nigeria.

This study is limited in a number of ways. Firstly, due to some inherent study limitations, there is some worry regarding variation that overstates or understate the relationship among variables, especially given the significant correrations that were observed between pairs of the three dimensions of cyber security efficacy. Secondly, perfect corroboration between bivariate and multivariate analyses was not achieved on the inference concerning moderating influence of topmanagement support. It was a deliberate design to use two layers of inferential analyses as a means of safey valve in drawing conclusions. While a reasonable degree of concurrence was achieved, it is worth noting that a less-than-100 per cent was achieved in this regard. Thirdly, the sampling did not take gender balance into account. Many different psychological and social factors affect employees' cybersecurity behaviors, (Anwar *et al.* 2016). It would be interesting to explore the extent to which gender plays a role in mediating the factors that affect cybersecurity beliefs and behaviors of employees in future research. Fourthly, this study made use of only one-sided opinion, which is that of Fintech companies. It would be interesting to carry out the same study but this time strictly from customers' perspectives. Future research is therefore encouraged to incorporate views from end users of Fintechs to have a balanced view. Lastly, the technical generalizability is limited by the omission of some key diagnostic evaluations and their possible impact on the result. For example, a study of this nature where cross sectional data was used is prone to heteroskedasticity,

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

a factor which was not taken into account. Besides, noticeable presence of multicollinearity were seen but ignored. Future studies might consider using robust standard errors instead of the OLS used in the current study.

5.2 Recommendations

Based on the results and conclusions, the following recommendations were made;

1) Fintech companies should improve on the use of multiple layer system of user ID authentication that includes bio-metric means. The conducted survey showed a weak prevalance of these authentication approaches, and yet access restriction capacity contributes the highest performance response coefficients.
2) Fintech companies should intensify efforts in the formulation and implementation of policy on Intrusion Detection and Prevention by installing Intrution Detection Sensors in their digital products. Again, the conducted survey showed this measure as the weakest of all the measures aimed at strengthening cyber attack resistance even though it is capable of eliciting positive performance response.
3) Fintech companies should enhance the capability of their products to automatically upgrade to newer or improved versions as soon as they become available. This is intended at eliminating or reducing replacement or upgrade implementation decision time lags due to beaurocratic bottlenecks associated with product quality reviews process from the end user.
4) Fintech companies that have products with lower access restriction capacity do not need top management support as much as those whose products exhibit higher access restriction capacity in order to enjoy high rate of return on their assets.

5.3 Contribution to Knowledge

This study has contributed to the literature in a number of ways. Firstly, the study enables the direct observation on how cyber security efficacy associates with financial performance. Unlike prior studies that offer indirect approach, this study provides a novel way to directly observe the nexus. Each of the dimensions of cyber security efficacy (i.e. access restriction to digital space, attack resistance capacity of digital space, and self-preservation capacity of digital space) offers a novel ways of dimensionalizing cyber security efficacy, thus contributing to the enrichment of literature on cyber security efficacy.

This study has produced evidence that each of these dimensions of cyber security efficacy has positive bearing on financial performance of Fintech companies in Nigeria. Prior to carrying out this study, there was no empirical evidence that links financial performance to cyber security efficacy directly.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

Reference

1) Adeyemi, Ehiwari & Dairo (2022). "*Nigeria Fintech Map & Year in Review*" An online catalogue of Fintech Companies. Accessed 07 April 2023

2) Akintoye, R; Ogunode, O.; Ajayi, M. & Joshua, A. A. (2022). Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. *Universal Journal of Accounting and Finance, 10*(3), 643-652. DOI: 10.13189/ujaf.2022.100302.

3) Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432–445.

4) Ali, L., Ali, F., Surendran, P. & Thomas, B. (2016). The effects of cyber threats n customer's behavior in e-banking services. *International Journal of e-Education, e-Business, E- Management and e-Learning, 7*(1), 70-77.

5) Anwar, Mohd & He, Wu & Ash, Ivan & Yuan, Xiaohong & Li, Ling & Xu, Li. (2016). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior. 69. 10.1016/j.chb.2016.12.040.

6) Bromiley P, McShane M, Nair A, & Rustambekov E (2014) Enterprise risk management: review, critique, and research directions. Long Range Plan 2(1):1–12. https://doi.org/10.1016/j.lrp.2014.07.005

7) Cavusoglu, H., Cavusoglu, H. & Zhang, J. (2008). Security patch management: Share the burden or share the damage?, *Management Science,* 54 (4), 657-670

8) Fahy, J & Smithee, A. (1999). Strategic marketing and the resource based view of the firm. *Academy of Marketing Science Review*, 3, 23-34.

9) Gordon, L.A. & loeb, A. (2006) Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective. Congressional Testimony.

10) Ibekwe, U. J., Agbaeze, E. K., Nwakoby, N. P., Abner, I. P., Kelvin-Iloafu, L. E., Akpan, E. E. (2019). Social media adoption and performance of telecommunication firms in Nigeria: From innovation diffusion theory to technology acceptance model. *International Journal of Mechanical Engineering and Technology*, 10(12), 100-114.

11) Khalil1, K.; Manzoor, S. R.; Tahir, M.; Khan, N. & Jamal, K. (2021). Impact of Cyber Security Cost on the Financial Performance of E-Banking: Mediating Influence of Product Innovation Performance. *Humanities & Social Sciences Reviews, 9*(2), 691-703

12) Klinle A, & Renn O (2011) Adaptive and integrative governance on risk and uncertainty. J Risk Res 15(3):273–292. https ://doi.org/10.1080/13669877.2011.63683 8

13) KPMG (2016) Risk governance: a benchmark analysis of systemically important banks. http://www.kpmg.com. Accessed 07 April 2023

14) Lowson, R. H. (2003). "The nature of an operations strategy: combining strategic decisions from the resource-based and market-driven viewpoints". Management Decision. 41 (6): 538– 549.

15) Njeru, P.W. & Gaitho, V. (2019). Investigating extent to which cybercrime influences performance of commercial banks in Kenya. International Journal of Economics, Commerce & Management, 8(8), 489 – 514.

16) Nweke, L.O. (2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal, 6(*12), 1-3.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 66 Issue 10| 2023
DOI: 10.5281/zenodo.10017426

17) Ojeka, S.A., Ben-Caleb, E. & EKpe, I. (2017). Cyber security in the Nigerian banking sector: An appraisal of audit committee effectiveness. International Review of Management and Marketing, 7(2), 340-346.

18) Pagach D, & Warr R (2011) The characteristics of firms that hire chief risk officers. J Risk Insur 78(1):185–211. https ://doi.org/10.2139/ssrn.1010200.

19) Rajendran V. (2018). Banking on its Security. *The Journal of Indian Institute of Banking& Finance, 89 (01),* 12-17.

20) Tumba, N.J., Onodugo, V.A., Akpan, E.E., & Babarinde, G.F. (2022). Financial literacy andbusiness performance among female micro-entrepreneurs. Investment Management and Financial Innovations, 19(1), 156-167. doi:10.21511/imfi.19(1).2022.12.

21) Yayla, A. A. & Hu, Q. (2011). The impact of information security events on the stock value of firms: the effect of contingency factors, *Journal of Information Technology*, 26 (1), 60-77.