Quantify the Maturity of Internet Banking Security Measures in WAEMU (West African Economic and Monetary Union) Banks

Marie Ndaw[1(✉)], Gervais Mendy[2], Samuel Ouya[2], and Diaraf Seck[2]

[1] GIM-UEMOA, Dakar, Senegal
lisandaw@gmail.com
[2] UCAD, ESP, LIRT, Dakar, Senegal
{gervais.mendy,samuel.ouya,diaraf.seck}@ucad.edu.sn

Abstract. WAEMU banks should provide more facilities and convenience to theirs customers but they also should take all steps and expensive measures to make online transactions more safe and secure. Several type of controls are proposed to manage different risks related to infiltrations, breaching, stealing data and cyber-attacks. Controls maturity are measured using the actual method which is manual, require time and personal investment and have some estimation error. In this paper, we propose and apply two models on all internet banking controls in order to automatize the quantification of their maturity. The both models allow optimal assessment of security measures and aim to improve security of Ebanking transactions including increase of comfort and time saving for underserved areas. The results of our study also enable economic/social well-being and financial inclusion to people in rural areas who use internet connection for mobile banking transactions.

Keywords: Internet banking · Risk · Security · Control

1 Introduction

Online banking is the use of the internet to deliver banking services such as funds transfer, paying bills, viewing current and savings account balance, purchasing financial instruments and certificates of deposits. The online services are easy to use, permit banking anytime, anywhere and anyhow and might differ from bank to bank. This facilitates all the functions and provide many advantages as compared to WAEMU traditional banking services but insecure channel such as the internet might not be the best base for bank customer relations as trust might partially be lost.

2 Literature Review

Several work are focused on Ebanking risk management. Sullivan in [1] showed that available risk measures may not capture the types of risk banks are exposed to with internet banking, such as security or operational risks. Abdou et al. in [2] concluded that the banks are working hard to mitigate the various risks. However, they cannot afford to

C. M. F. Kebe et al. (Eds.): InterSol 2017/CNRIA 2017, LNICST 204, pp. 125–130, 2018.
https://doi.org/10.1007/978-3-319-72965-7_11

become complacent when considering the adverse impact of increasing customer complaints, financial data, news headlines, corporate governance issues and credit crunch fall out which are all potentially critical of their risk control measures. Drimer et al. [3] showed that Bank website includes a prefix which customizes the user prompts and reduces the risk of social engineering because the field descriptions are more specific.

Different types of attack exist and should be addressed by banks in order to improve the online transaction security. Weest in [4] classified E-banking attacks into three categories: Local attacks, Remote Attacks and Fraud Prevention Technologies. Otsuka in [5] related the Federal Financial Institutions Examination Council issued updated authentication guidance which suggest to reinforces and stresses the importance of performing periodic risk assessment and implement layered security controls at various points in the transaction process.

Banks shoul implement appropriate controls by taking into account different types of Ebanking risks; Ting et al. research [6] disclosed new frameworks which state that the financial risk, time risk, security risk, performance risk and social risk have a significant relationship towards consumers behavioral intention to use online banking. Zarei in [7] showed that Banks must be conscious of different types of risks related to Ebanking: Cross border risks, Security risks, Legal and Ethical risks, Operational risks, Reputational Risks, Strategic risks, Money laundering risks and Traditional risks. Li et al. in [8] related that online auction sites often claim that they have no control over the quality, safety or legality of the items advertised, the truth or accuracy of the listings, thus exposing bidders to potential risks and fraudulent transactions. Malhotra and Singh in [9] showed that Internet banking has a negative and significant impact on risk which shows that its adoption has increased the risk profile of banks. So its necessary to apply efficacy security measures at different level. Hole et al. in [10] concluded that the popularity of online Banking has attracted the internet criminals to attack online Banking customers. Sarma and Singh in [11] related that biometric technology has played an important role to control the risk factors through Authentication system. The implementation of appropriate authentication methodologies should start with an assessment of the risks faced by the Internet banking systems. Security measures should also concern customers. In [12], severals guidelines for safe online banking are proposed. Osunmuyiwa in [13] proposed others guidelines like never click on links or applications that you receive in emails or text messages and avoid using unsecured public wireless connections.

3 Problem

We have noted that WAEMU banks use different types of measures to secure online transactions and periodically assess their risks by calculating residual criticality. Jenkins in [14] related that the residual criticality gives an appreciation of the impact of implemented controls on identified risks. Lipol and Haq in [15] showed that it is obtained by estimation of maturity of the implemented controls on risk criticality. Exposure of WAEMU banks is clearly increasing, raising new possibly systemic risks [16]. Africa country gets broadband connectivity, usually without adequate defenses, cybercrime

spikes within a few days. The regional effect is significant because less-developed countries are more vulnerable [17]. The actual used method for assessing controls maturity is manual and has some limits including: time and personal investment, different appreciation of maturity. Controls assessment is difficult and not automatized; this may cause unsecured online transitions, loss of customer confidence for underserved areas customers.

4 Our Contribution

We propose to automatize calculation of controls maturity by defining two models which allow automatic calculation of controls maturity. For this, we work with WAEMU banks which offer traditional banking services and electronic banking products like withdrawal, payment using credit, debit or prepaid card, E-banking and M-banking. We also take into account all local banking regulations for WAEMU banks, safety standards of information system and electronic banking, collaborations and partnerships. This sample is representative because other banks have approximately the same risk considering their similar activity, infrastructure and their dependance on local laws and regulations. The two models are finally tested on controls related to type of information system component and type of Ebanking risks. The results are satisfactory for both models and suggest to choose the second which have the best correlation rate with estimation and is very easy to use.

4.1 Models Principles

To propose those models, we used the following 7 principles:

- Principle 1: Risk may have one or more controls
- Principle 2: Control is defined to treat the identified and assessed risks
- Principle 3: Control have one maturity and three types (preventive, detective or corrective)
- Principle 4: Only mature control can reduce likelihood and severity of risk
- Principle 5: Preventive control may reduce the likelihood of the risk (P)
- Principle 6: Detective control may reduce severity of the risk (G).
- Principle 7: Corrective control may reduce severity of the risk (G)

4.2 The Proposed Models

Model 1: The fist proposed model is declines as follows:

$$Maturity_{controls} = \left[\left(\sum_{1}^{ni} (a_i * i) + \sum_{1}^{nj} (a_j * j) + \sum_{1}^{nk} (a_k * k) \right) \Big/ (ni + nj + nk) \right] \quad (1)$$

The first model has six independent parameters:

- [a_i][a_j][a_j]: *Maturity Index of preventive detective and corrective controls*
- [i] [j] [k]: prevention detective corrective index

And depends on 3 independent variables:

ni [nj][nk]: number of preventive detective corrective controls.

Model 2: The second proposed model which calculate residual criticality is declines as follows:

$$Maturity_{controls} = \left[MatCoef * \left(\sum_{1}^{n_{ctl}} (mat_i) \Big/ n_{ctl} \right) \right] \quad (2)$$

For each characteristic, we have defined a impact percentage based on 10 main characteristics of control maturity in order to obtain a maturity coefficient (Table 1):

Table 1. Main characteristics of control

Level	Characteristics	Percentage
1	Exits	10%
2	Exits and Documented	15%
3	Exits, Documented and Executed	35%
4	Exits, Documented, Executed and Traceable	45%
5	Exits, Documented, Executed, Traceable and Effective	55%
6	Exits, Documented, Executed, Traceable, Effective and Efficient	65%
7	Exits, Documented, Executed, Traceable, Effective, Efficient and Self-assessed	75%
8	Exits, Documented, Executed, Traceable, Effective, Efficient, Self-assessed and Managed	85%
9	Exits, Documented, Executed, Traceable, Effective, Efficient, Self-assessed, Managed and Reported	95%
10	Exits, Documented, Executed, Traceable, Effective, Efficient, Self-assessed, Managed, Reported and Archived	100%

Maturity Coefficient (MatCoef = 0.1); Control maturity($[mat_i] = [1, 2, 3, 4, 5]$) Number of Control ($[n_{ctl}] = [1, 2, 3]$).

Models advantages: The two proposed models are innovation and have several advantages including: optimal assessment of security measures, automatic calculation of controls maturity, decrease of estimation error rate, reduced time for obtaining controls maturity. Also This result help to improve online transactions security, increase customer confidence, comfort and time saving. Otherwise, secure internet connection allow mobile payment which enable financial inclusion and payments system efficiency for rural people.

4.3 Tests

Application of two models on all controls: We apply the two models on all E-banking controls using the defined formulas.

Application of two models on controls by type of to information system component: We test the models on controls by type of information system component as indicated in the below graph (Fig. 1):

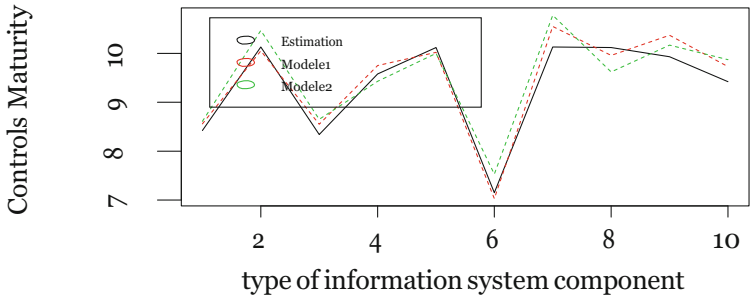

Fig. 1. Controls maturity by type of information system component

Results 1

- Models values are equal, upper or lower than estimation values
- Residual values between models and estimation are random
- Correlation rate with estimation values is 96% for model 1 and 97.5% for model 2
- Model 1 have more parameters than Model 2 which is more easier

Application of the model on controls by type of Ebanking risks. We also test the model on controls by type of Ebanking risks as indicated in the below graph (Fig. 2):

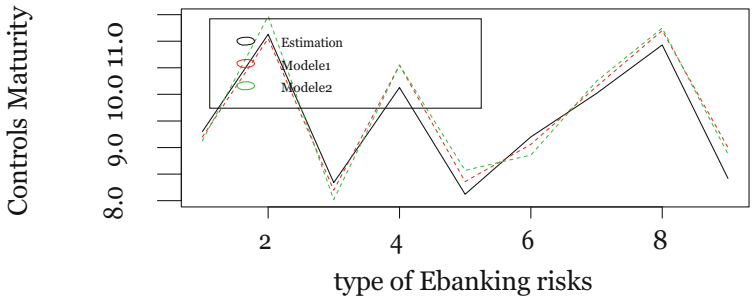

Fig. 2. Controls maturity by type of Ebanking risks

Results 2

- Models values are equal, upper or lower than estimation values
- Residual values between models and estimation are random
- Correlation rate with estimation values is 95% for model 1 and 97% for model 2
- Model 1 have more parameters than Model 2 which is more easier

5 Conclusion

The online banking provides many benefits to WAEMU customers but it also aggravates traditional banking risks. Increased use of mobile services and internet as a new distribution channel for WAEMU banking transactions requires more attention against fraudulent activities. Our study was taken with an objective to define and test two models for calculation of online banking controls maturity. The models values were compared to estimation values given by interlocutors during the traditional working sessions. The both models allow an automatic calculation of Ebanking controls maturity, help to increase WAEMU banks profit and enable convenience and flexibility for underserved area. After testing and comparison, Model 2 has better correlation rate and is very easy to implement. In our future works, we will apply the two models on mobile banking and mobile payment risks.

References

1. Sullivan, R.J.: How has the adoption of internet banking affected performance and risk in banks. Financial Industry Perspectives (2000)
2. Abdou, H., English, J., Adewunmi, P.: An investigation of risk management practices in electronic banking (2014)
3. Drimer, S., Murdoch, S.J., Anderson, R.: Optimised to fail: card readers for online banking. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 184–200. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03549-4_11
4. Weest, C.: Threats to Online Banking. Symantec Security Response, Dublin (2005)
5. Otsuka, K.: Online Banking Risk eFraud: Hands off my Account. CPA Risk Management, CUNA Mutual Group (2011)
6. Ting, A.H., Kuen, F.S., Xien, G.L., Ying, L.Y., Yew, W.S.: Online banking in Malaysia from consumer perception on risk, April 2013
7. Zarei, S.: Risk Management of Internet Banking, Iran (2011). ISBN: 978-960-474-273-8
8. Li, H., Ward, R., Zhang, H.: Risk, Convenience, Cost and Online Payment Choice: A Study of eBay Transactions. Georgia Institute of Technology, Atlanta
9. Malhotra, P., Singh, B.: The impact of internet banking on bank performance and risk. Eurasian J. Bus. Econ. **2**(4), 43–62 (2009)
10. Zhang, F.: An Analysis of the Online Banking Security Issues Reported by, Hole, Moen, Tjostheim. University of Auckland
11. Sarma, G., Singh, P.K.: Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. ISSN 2229 - 6107
12. Risk Mitigation Best Practices for Mobile and Online Banking, State Bank of Belle Plaine Consumers
13. Osunmuyiwa, O.: Online Banking and the Risks Involved (2013)
14. Koffi, W.S.: The Fintech Revolution: An Opportunity for the West African Financial Sector. School of Economics (2016)
15. Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II, June 2014
16. Jenkins, B.: Risk Analysis helps establish a good security posture (1998)
17. Lipol, L., Haq, J.: Risk Analysis Method: FMEA/FMECA in the Organizations. University of Boras, Sweden (2011)