

Bank Customer Service Dynamic Survey for Quantitative Risk Assessment and Cost Effective Management

M. Sahinoglu, P. Vasudev, S. Morton

Auburn University at Montgomery (AUM), Montgomery

mesa@aum.edu, pvasudev@aum.edu, smorton1@aum.edu

Abstract: Risk assessment and management is of critical importance to modern enterprises and organizations. Bank Customer Service risk is concerned primarily with how customers of a bank rate their experience with the various aspects of banking. In the current financial conditions and competition among banks, it's easy for customers to switch if they are not satisfied. This risk related to bank customer can be assessed by investigating various aspects of banking activities. The principal author has built the foundational aspects and an associated automated software tool for quantitative risk management. This software tool, the Risk-o-Meter (RoM) will provide measurable risk, cost, and risk mitigation advice for vulnerabilities associated with banking.

I. INTRODUCTION

There are few customer satisfaction surveys like sogosurvey.com [1], but these are qualitative based. There are guidelines on how to choose metrics [2] and also research related to customer service and retail banking [3] is available, but there is no definitive framework to capture data and analyze it. Wiki defines Risk as 'the potential of losing something of value, weighed against the potential to gain something of value'. In the context of banking, customer relationship is valuable; hence it pays to manage the associated risks by identifying threats and vulnerabilities. Once all risks are identified, formulating a cost-optimized solution to mitigate undesirable risks to a tolerable level is often an ad-hoc process. In this research, we adopt a model of customer satisfaction risk that quantifies the user's experience with five crucial aspects of the banking. However we will add an original concept of quantification to the existing model through a designed algorithm by the principal author to calculate the bank customer satisfaction risk index. To accomplish this task, numerical and/or cognitive data was collected to supply the input parameters to calculate the quantitative satisfaction risk index for a given bank. This paper will not only present a quantitative model but also provide a remedial cost-optimized game-theoretic analysis about how to bring an undesirable risk down to a locally-determined "tolerable level".

II. METHODOLOGY

This applied research paper implements a methodology on how to reduce the risk associated with bank customer service with respect to given bank. A Software-centered composite security posture is proposed to aid bank management, staff, and call-center reps within a bank. The primary author's innovation, i.e. RoM (Risk-O-Meter), an automated software tool, will provide bank managers a measurable assessment of the current service level detailing associated cost and risk mitigation suggestions for identified vulnerabilities and threats associated with the overall banking experience, from customer's perspective. The Risk of Service (RoS) metric out of 100% will be assessed and provide a remedial cost-optimized game-theoretic analysis about how to bring an undesirable risk down to a locally-determined "tolerable level". While the Risk-O-Meter can be utilized on virtually any aspect of business, this particular implementation focuses on five key areas critical in ensuring Bank Customer Service Satisfaction.

1. Access Modes: Very first step in banking is to get in touch with the bank. Advent of telephone and internet has affected banking domain too. Customers expect convenience, be it ability to do online banking from home or work, drive-through ATMs for quick cash withdrawal, etc, etc. This key area focuses on Online Presence, Telephone Communication, and Branch or ATM location. Each of these areas must be addressed to meet needs of customers of every generation.
2. Branch Experience: Many customers still prefer traditional way of banking which adds a personal touch. This is particularly important for those customers who manage many account related to various aspects like debit accounts, loans, mortgages, wealth management, etc with same bank. This vulnerability covers Customer Reception, Information Availability, Branch Ambiance, and Waiting Time.
3. Customer Service: This includes general Customer Service related areas like Customer Friendliness of customer service reps or staff at branch, way in which Collections are handled, Familiarity or Knowledge level of service reps with respect to bank offerings, and Business Hours.
4. Transactions: Once bank-customer relationship has been established, focus moves to Transactions. Is Fee reasonable & comparable to other banks? Does Processing Time match or exceed that of competitor banks? Are there any functional glitches in Interbank Communication? Is International Banking facilitated?
5. Products & Services: This area of interest looks at Products offered by bank in different domains like savings, investments, insurance, mortgages & loans. Services assessed include bank proactively sending monthly statements, providing conveniences like (auto) bill-pay, financial planner app / calendar, automatically renewing expired cards, monitoring transactions to thwart fraud payments, etc. How about Compliance? Is customer assured of their deposit money? Is Privacy handled with due diligence? Is bank involved in local community? Online Banking section delves deep to assess CIA related to online banking.

This research focuses on the areas vital to ensure customer service provides bank managers with an analysis they can use to more efficiently serve their customers.

III. VULNERABILITIES, THREATS AND COUNTERMEASURES

As previously noted, five vulnerabilities are assessed: Access Modes, Branch Experience, Customer Service, Transactions, and Products & Services. Within each vulnerability category, questions pertain to specific threats and countermeasures. For example, within the Branch Experience vulnerability, users are asked questions regarding Ambiance, Waiting Times, Information Availability and Customer Reception threats and countermeasures. See Figure 1 regarding Bank Customer Service Satisfaction Risk Diagram below for all associated vulnerabilities and threats. The users' responses are then used to generate a quantitative bank customer service risk index.

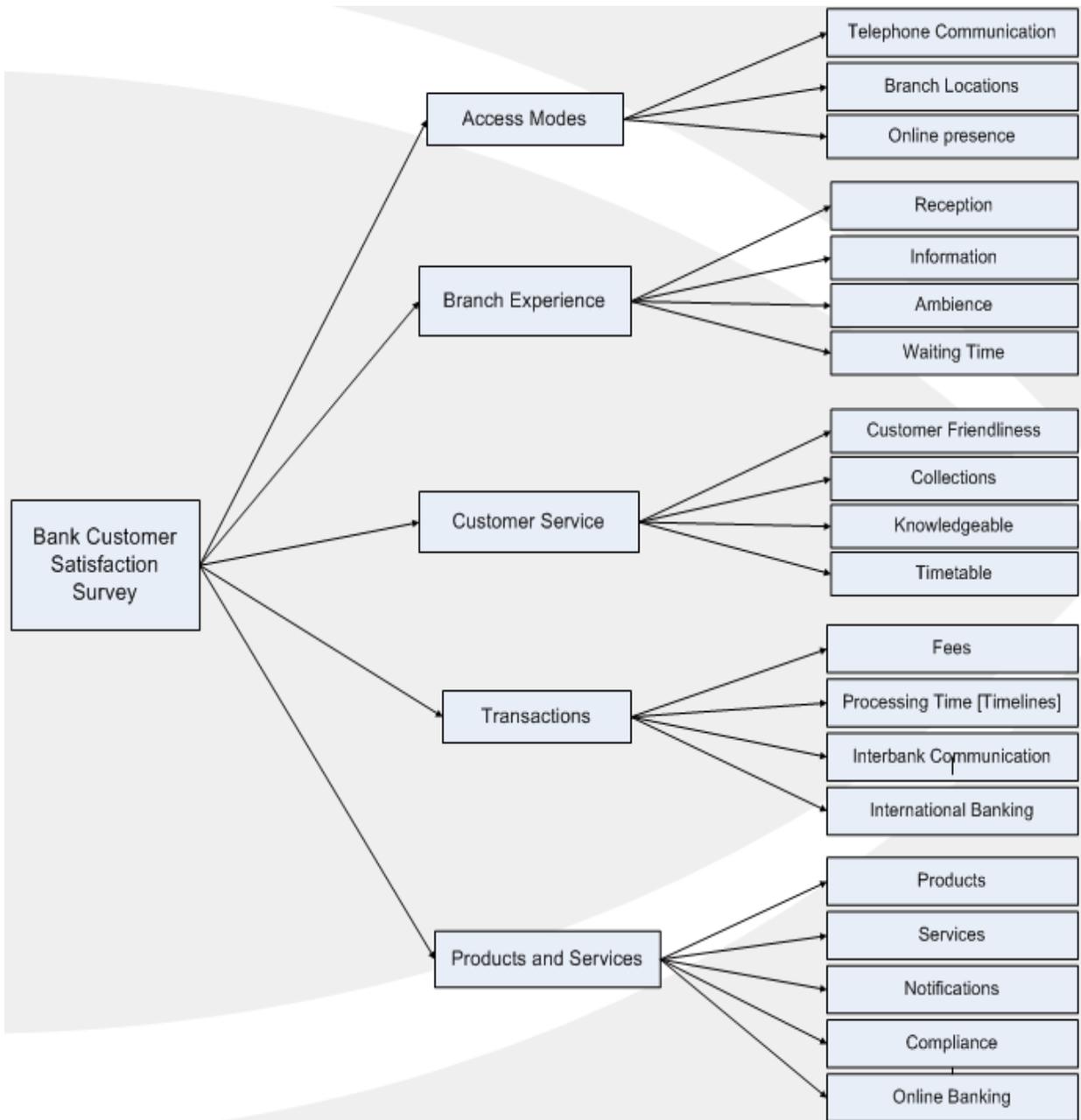


Figure 1. Bank Customer Service Satisfaction Risk Diagram
 IV. ASSESSMENT QUESTIONS

Questions are designed to elicit the user's response regarding the perceived risk from particular threats, and the countermeasures the users may employ to counteract those threats. For example, in the Products and Services vulnerability, questions regarding Online Banking include both Threat and Countermeasure questions.

Threat questions would include:

- Is bank website not secure?
- Is it unsafe if user forgets to explicitly logout after online banking?
- Is it easy to break customer login (authentication)?
- Is bank website down often times?
- Does customer need to login multiple times for different accounts?

While countermeasure questions would include:

- Are branch transactions done over secure connections like https or ssl?
- Is Digital Certificate valid and current?
- Does online session expire automatically after few minutes of inactivity?
- Does bank employ Multi-factor authentication?
- Does bank ensure online banking is available 24/7?
- Does bank ensure all debit/credit/loan accounts are accessible from one online account?

Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res Risk	Change	Opt Cost	Unit Cost	Final Cost	Advice
0.562500	1.000000	0.750000		0.999950		0.249950	\$129.41			Increase the CM capacity for threat "Bank or ATM Locations" for the vulnerability of "Ease of Access" from 75.00% to 100.00% for an improvement of 25.00%. Increase the CM capacity for threat "Processing time" for the vulnerability of "Transactions" from 17.50% to 31.44% for an improvement of 13.94%.
		0.250000	0.140625	0.000050	0.000028					
0.437500	1.000000	0.175000		0.314350		0.139350	\$72.15			
		0.825000	0.360937	0.685650	0.299972					
						Total Change	Total Cost	Break Even Cost	Total Final Cost	
						38.93%	\$201.56	\$5.18		

Criticality	1.00	Total Risk	0.501562	Total Risk	0.300000
Capital Cost	\$1,000.00	Percentage	50.156250	Percentage	30.000002
Total Threat Costs	N/A	Final Risk	0.501562	Final Risk	0.300000
		ECL	\$501.56	ECL	\$300.00
				ECL Delta	\$201.56

<input type="button" value="Change Cost"/>	<input type="button" value="Change Unit Cost"/>
<input type="button" value="Show where you are in Security Meter"/>	<input type="button" value="Calculate Final Cost"/>
<input type="button" value="Optimize"/>	<input type="button" value="Print Summary"/>
	<input type="button" value="Print Results Table"/>
	<input type="button" value="View Threat Advice"/>
	<input type="button" value="Print Single Threat/CM Selection"/>
	<input type="button" value="Print Advice Threat/CM Selections"/>
	<input type="button" value="Print All Threat/CM Selections"/>
	<input type="button" value="Update Survey Questions"/>

2 Vulnerabilities

Figure 2. Bank Customer Service Satisfaction – Optimization Screenshot
V. RISK CALCULATION AND MITIGATION

Essentially, the users are responding Yes or No to these questions. These responses (approximately normally distributed since Mean and Median are almost the same) are used to calculate residual risk. Using a game-theoretical mathematical approach, the calculated risk index is used to generate an optimization or lowering of risk to desired levels [4]. Further, mitigation advice will be generated to show bank managers, branch staff, customer service reps, and other interested parties [5]. That is, in what areas the risk can be reduced to optimized or desired levels such as from 50% to 30% in the screenshot representing the median response from the study participants.

Figure 2 above is a screenshot of the Median Risk Meter Results Table displaying threat, countermeasure, and residual risk indices; optimization options; as well as risk mitigation advice. For this study, a random sample of 31 respondents was taken and their final risk percent results are tabulated and presented in Appendix A and B with details at the end of this paper.

VI. CONCLUSION

The Risk Meter breaks new ground in that it provides a quantitative assessment of risk to the user as well as recommendations for mitigating that risk. As such, it will be a highly useful tool for security personnel, facility managers, network personnel, management, and other interested parties seeking to minimize and mitigate bank customer service risk in an objective, quantitatively based manner. Future work will involve the incorporation of new questions so as to better refine user responses and subsequent calculation of risk and mitigation recommendations. Minimization and mitigation of bank customer service risk will greatly benefit not only the organizations deploying the applications, but society at large through the minimization of security breaches leading to monetary loss and ID theft.

VII. REFERENCES

- [1] <http://www.sogosurvey.com/sample-surveys.aspx>
- [2] <http://www.howto.gov/customer-experience/models/customer-experience-model/exceed-expectations>
- [3] Customer satisfaction and retail banking: an assessment of some of the key antecedents of customer satisfaction in retail banking, Ahmad Jamal, (Cardiff Business School, Cardiff, UK), Kamal Naser, (Cardiff Business School, Cardiff, UK), <http://www.emeraldinsight.com/journals.htm?articleid=855059&show=abstract>
- [4] M. Sahinoglu, Trustworthy Computing, John Wiley, 2007.
- [5] M. Sahinoglu, “An Input-Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk”, IEEE Transactions on Instrumentation and Measurement, Vol. 57, No. 6, pp. 1251-1260, June 2008.

APPENDIX A: Respondent Final Risk Percent Results Table

Bank	Survey Taker	Final Risk %	
ASECU	ASECU_01	45.86	
Auburn Bank	Auburn_01	46.44	
BBVAC	BBVAC_01	53.34	
	BBVAC_02	43.67	
BCS	BCS_01	44.68	
	BCS_02	38.24	
	BCS_03	65.56	
BOA	BOA_01	55.08	
	BOA_02	53.81	
GCU	GCU_01	53.61	
Max CU	MaxCU_01	53.15	
	MaxCU_02	52.75	
	MaxCU_03	51.65	
	MaxCU_04	78.33	
	MaxCU_05	51.47	
Max Fed	MaxFed_01	42.38	
	MaxFed_02	37.85	
Regions	Regions_01	38.90	
	Regions_02	42.20	
	Regions_03	39.51	
	Regions_04	44.80	
	Regions_05	40.19	
	Regions_06	70.26	
	Regions_07	45.55	
	Regions_08	51.88	
USAA	USAA_01	50.16	Median
	USAA_02	41.16	
WF	WF_01	61.14	
	WF_02	70.29	
	WF_03	57.11	
	WF_04	45.95	
	Median	50.16	
	Mean	50.55	

APPENDIX B: Bank Survey Details

Bank Customer Service Risk survey has 5 categories of areas of interest (vulnerabilities) related to banking from customer's perspective as listed in Risk Diagram.

Directions:

This Page:

- Enter your name (optional)
- Enter bank name (mandatory)
- Select all vulnerability areas that apply
- Proceed to appropriate pages to complete survey for respective vulnerability

Survey Page(s):

1. Vulnerability:

- Rate Vulnerability (1-10) with 10 being most vulnerable and 1 being least vulnerable
- Tick/mark all checkboxes that apply

2. Threat:

- Rate Threat (1-10) with 10 being greatest threat and 1 being least threat
- Tick/mark each threat for each threat category (must choose atleast one)

3. Counter Measures:

- Rate associated Counter Measure (1-10) for each threat category chosen above with 10 being most effective and 1 being least effective
- Tick/mark each threat for each threat category (must choose atleast one)

Name: Jane Doe

Bank: PoorPeoplesBank

Vulnerability Area		Reference Page
<input type="checkbox"/>	Access Modes	Page 4
<input type="checkbox"/>	Branch Experience	Page 5
<input type="checkbox"/>	Customer Service	Page 6
<input type="checkbox"/>	Transactions	Page 7
<input type="checkbox"/>	Products and Services	Pages 8, 9

Vulnerability: Access Modes
<input type="checkbox"/> Contacting bank online / online presence <input type="checkbox"/> Telephone Communication <input type="checkbox"/> Branch / ATM locations

Threat: Online Presence	CounterMeasures
<input type="checkbox"/> Is the customer unable to locate bank information on the internet? <input type="checkbox"/> Is the customer unable to do bank transactions online? <input type="checkbox"/> Is the customer unable to search for bank branches on its website? <input type="checkbox"/> Is bank website slow to load? <input type="checkbox"/> Does bank website fail to load in browsers other than Internet Explorer?	<input type="checkbox"/> Is the bank URL displayed in search results of major search engines? <input type="checkbox"/> Does the bank support online banking? <input type="checkbox"/> Can customer look-up branch location online? <input type="checkbox"/> Does the website provide contact info for all branches? <input type="checkbox"/> Are all links in the bank website working? <input type="checkbox"/> Is bank website URL intuitive ie., same as bank name? <input type="checkbox"/> Does bank website support major browsers like chrome, firefox, etc ?

Threat: Telephone Communication	CounterMeasures
<input type="checkbox"/> Are the bank contact numbers difficult to find? <input type="checkbox"/> Are the listed bank contact numbers invalid? <input type="checkbox"/> Are phone-banking services different from online services? <input type="checkbox"/> Does the customer need to pay for phone-banking?	<input type="checkbox"/> Are customers given list of bank contact numbers when they open account? <input type="checkbox"/> Are the listed contact numbers answered during business hours? <input type="checkbox"/> Are the listed contact numbers working? <input type="checkbox"/> Is phone-banking services at par with online services? <input type="checkbox"/> Is phone-banking free of charge?

Threat: Branch or ATM Locations	CounterMeasures
<input type="checkbox"/> Do customers travel long distance to reach bank location? <input type="checkbox"/> Are there no branches in your city or town? <input type="checkbox"/> Are branches situated away from town centers or shopping malls? <input type="checkbox"/> Is there a parking problem at the branches?	<input type="checkbox"/> Are there branches in each county? <input type="checkbox"/> Are there branches/ATMs within 15-mile radius of work or home? <input type="checkbox"/> Are branches situated in vicinities of shopping centers? <input type="checkbox"/> Do all branches have abundant parking areas?

Vulnerability: Branch Experience

- Is there no reception at branch?
- Are information packs, display boards missing?
- Is the ambiance unpleasant?
- Is it long waiting time?

Threat: Reception

- Is there a differential treatment for customers based on color, gender, etc ?
- Does the customer feel unwelcome?
- Does the customer feel hesitant to ask questions?
- Do customers have to get out of car and enter branch for day-to-day banking?

CounterMeasures

- Are all customers treated in a same way?
- Is there a receptionist to welcome customers?
- Is the receptionist customer friendly?
- Can customers do banking via drive-through?
- Do bank employees answer all queries in good manner?

Threat: Information

- Is information on even everyday activities not displayed?
- Do customers have to ask for account related information?
- Is branch business hours not displayed?
- Is information printed only in English?

CounterMeasures

- Are leaflets on day-to-day activities placed at strategic locations?
- Are current and savings rate, loan interest rate, etc displayed?
- Is branch working hours displayed near the entrance?
- Is information available in language other than English?

Threat: Ambiance

- Is it too hot or too cold inside branch?
- Are coffee, juices, water and snacks unavailable?
- Is there nothing to read or do while waiting to be served?
- Is there no seating arrangement for waiting customers?

CounterMeasures

- Is the room temperature monitored?
- Are beverages and snacks available for customers?
- Is the branch well appointed with much light and space?
- Are periodicals and TV available for clients?
- Are there ample seats for waiting customers and customers being served?

Threat: Waiting Time

- Do customers wait for long time before being served?
- Do customers wait for long time to get task done?
- Do customers wait in long queues in drive-through?
- Do customers wait in long queues at ATMs?

CounterMeasures

- Are there sufficient tellers to attend clients in a timely manner?
- Are workflows sufficiently streamlined to ensure minimal transaction time?
- Are there atleast couple of drive-throughs at each branch?
- Are there atleast two ATMs at each branch?

Vulnerability: Customer Service

- Does customer service handle collections impolitely?
- Is customer service hostile towards customer ?
- Are customer service agents less knowledgeable about bank, services and procedures?
- Is the branch working hours inconvenient for customers?

Threat: Collections

- Do collections reps call up customers before grace period ends?
- Are reps rude when reminding customers about pending payments?
- Is there no reminder mechanism for upcoming payments?
- Is there no mechanism automating payments?

CounterMeasures

- Are reps instructed not to call before the grace period ends?
- Are reps professional when reminding customers about overdue payments?
- Are customers reminded of their upcoming payments by mail or email?
- Is there an auto-debit facility for payments?

Threat: Customer Friendliness

- Are customer service reps rude or unprofessional?
- Do customer service reps hang-up on customers?
- Are customer service reps overly familiar?
- Do customer service reps deal with multiple customers at same time?

CounterMeasures

- Are customer service reps trained to be polite and professional?
- Do customer service reps ensure all customer queries are answered satisfactorily?
- Do customer service reps engage only in business related conversation?
- Do customer service reps handle one customer at a time?

Threat: Knowledgeable

- Are customer service reps unaware of products offered by bank?
- Are customer service reps unable to handle customer queries?
- Are customer service reps unable to understand customer needs?
- Are customer service reps unable to suggest alternatives?

CounterMeasures

- Are customer service reps made aware of all products and services offered by bank?
- Are customer service reps trained to handle customer queries in a thorough manner?
- Do customer service reps have customer service education or background?
- Do customer service reps provide the customer with all necessary information?

Threat: Business Hours

- Is the branch hours vary from day to day?
- Does the branch open late in morning?
- Does the branch close too early in evening?
- Is the branch closed during general lunch hours?
- Are customers unable to use ATMs on weekends?

CounterMeasures

- Are branch hours the same on all working days?
- Does the branch open before 9am?
- Is the branch open until 6pm?
- Does the branch serve customers during general lunch hours?
- Does the branch ensure ATMs are functional on weekends?

Vulnerability: Transactions	
<input type="checkbox"/> Are service charges unreasonable? <input type="checkbox"/> Is processing time unreasonable? <input type="checkbox"/> Are transactions with other branches not in harmony? <input type="checkbox"/> Are overseas transactions not handled well?	
Threat: Fees	CounterMeasures
<input type="checkbox"/> Is minimum balance required in checking or savings account too high compared to other banks? <input type="checkbox"/> Is penalty for late payment too high? <input type="checkbox"/> Is penalty for bounced cheques too high? <input type="checkbox"/> Is charge for ATM card usage with other bank too high? <input type="checkbox"/> Is interest paid on savings account too less?	<input type="checkbox"/> Is minimum balance required in checking or savings account as per local regulations? <input type="checkbox"/> Is penalty for late payment as per local guidelines and regulations? <input type="checkbox"/> Is ATM card usage at other banks charged reasonably? <input type="checkbox"/> Is interest offered on savings or checking account on par with other banks?
Threat: Processing time	CounterMeasures
<input type="checkbox"/> Does opening or closing an account take more than one hour? <input type="checkbox"/> Does it take weeks for loan processing? <input type="checkbox"/> Does it take too many days for checks to clear? <input type="checkbox"/> Does it take more than one business day for online payment processing?	<input type="checkbox"/> Is opening or closing or any account related activity a matter of minutes? <input type="checkbox"/> Is loan application processed within couple days? <input type="checkbox"/> Are checks cleared in less than 24 hours? <input type="checkbox"/> Is online payment processing instant?
Threat: Interbank communication	CounterMeasures
<input type="checkbox"/> Are customers unable to transfer money to customers of other banks? <input type="checkbox"/> Are customers double charged (once by each bank) for day-to-day banking activities? <input type="checkbox"/> Are interbank transaction fees too high? <input type="checkbox"/> Is interbank transaction processing time too long?	<input type="checkbox"/> Can customer transfer money online or by telephone banking to customers of other banks? <input type="checkbox"/> Is money inflow into account free of charge? <input type="checkbox"/> Is interbank transaction fee reasonable and in-line with local guidelines and regulations? <input type="checkbox"/> Is interbank transaction time comparable to normal transaction processing time?
Threat: International Banking	CounterMeasures
<input type="checkbox"/> Are customers unable to transfer money overseas? <input type="checkbox"/> Are international banking charges too high? <input type="checkbox"/> Is international transaction processing time too long? <input type="checkbox"/> Is currency exchange rate way off the market rate?	<input type="checkbox"/> Can customer transfer money online or by telephone banking overseas? <input type="checkbox"/> Is international transaction fee reasonable and comparable to other banks? <input type="checkbox"/> Is international transaction time reasonable and take time-zone into account? <input type="checkbox"/> Is currency exchange rate offered inline with market rate?

Vulnerability: Products and Services
<input type="checkbox"/> Are the products or services offered limited? <input type="checkbox"/> Does the branch offer inferior services compared to other banks? <input type="checkbox"/> Does the bank miss to send notifications or statements? <input type="checkbox"/> Does bank fail to comply to FFIEC regulations? <input type="checkbox"/> Is bank's website not very user-friendly?

Threat: Products	CounterMeasures
<input type="checkbox"/> Does the bank offer only plain vanilla account type? <input type="checkbox"/> Does the bank offer only one type of loan? <input type="checkbox"/> Does the bank offer only a single investment option? <input type="checkbox"/> Does the bank offer only one type of insurance?	<input type="checkbox"/> Does the bank offer various account types like savings, current, recurring, e-saver, etc? <input type="checkbox"/> Does the bank offer various loans like home loan, personal loan, auto loan, etc? <input type="checkbox"/> Does the bank offer various investment options like shares, bonds, ETFs, etc? <input type="checkbox"/> Does the bank offer various insurance options like auto, home, house-owner, etc?

Threat: Services	CounterMeasures
<input type="checkbox"/> Is it a laborious process to manage various accounts? <input type="checkbox"/> Is it cumbersome to manage bill payment? <input type="checkbox"/> Does customer need to be approach bank to renew expired debit cards? <input type="checkbox"/> Does customer need to file monthly paper account statements for future reference?	<input type="checkbox"/> Does bank offer easy way to manage all accounts like savings, loan, etc at one place? <input type="checkbox"/> Does bank offer easy way to pay all bills from one centralized account? <input type="checkbox"/> Does bank proactively issue new cards when debit cards are about to expire? <input type="checkbox"/> Does bank provide facility to view past monthly account statements?

Threat: Notifications	CounterMeasures
<input type="checkbox"/> Does bank miss out sending monthly statements? <input type="checkbox"/> Does bank miss out sending changes to agreements? <input type="checkbox"/> Is bank irregular in sending tax related 1099* forms? <input type="checkbox"/> Do branches change working hours without prior notification to customers?	<input type="checkbox"/> Does bank issue monthly statements regularly? <input type="checkbox"/> Does bank notify customers about changes to policies and user agreements? <input type="checkbox"/> Does bank send annual forms like 1099*, etc on time? <input type="checkbox"/> Do branches notify customers of changes to working hours, etc well in advance?

Threat: Compliance	CounterMeasures
<input type="checkbox"/> Is Privacy statement missing? <input type="checkbox"/> Is it easy channel money through various anonymous sources(money laundering)? <input type="checkbox"/> Are customers forced to buy products like credit card insurance? <input type="checkbox"/> Is there no assurance for customers with respect to their deposits? <input type="checkbox"/> Does bank shy away from Community involvement ?	<input type="checkbox"/> Does bank disclose its Privacy policy? <input type="checkbox"/> Does bank follow FFIEC guidelines related to anti-money laundering and anti-terrorism? <input type="checkbox"/> Does bank follow implement sufficient checks to counter money laundering? <input type="checkbox"/> Does bank invest in community as per Community Reinvestment Act? <input type="checkbox"/> Are customers covered under FDIC insurance?

Vulnerability: Products and Services

Threat: Online Banking	CounterMeasures
<ul style="list-style-type: none"><input type="checkbox"/> Is bank website not secure?<input type="checkbox"/> Is it unsafe if user forgets to explicitly logout after online banking?<input type="checkbox"/> Is it easy to break customer login (authentication)?<input type="checkbox"/> Is bank website down often times?<input type="checkbox"/> Does customer need to login multiple times for different accounts?<input type="checkbox"/> Does customer need to maintain multiple accounts for different account types?	<ul style="list-style-type: none"><input type="checkbox"/> Are branch transactions done over secure connections like https?<input type="checkbox"/> Is Digital Signature valid and current?<input type="checkbox"/> Does online session expire automatically after few minutes of inactivity?<input type="checkbox"/> Does bank employ Multi-factor authentication?<input type="checkbox"/> Does bank ensure online banking is available 24/7?<input type="checkbox"/> Does bank ensure all debit/credit/loan accounts are accessible from one online account?

About the Authors:

Dr. M. Sahinoglu is the founding Director of the Informatics Institute and Head, Cybersystems and Information Security Graduate Program at Auburn University at Montgomery (AUM). Formerly, the Eminent Scholar and Chair-Professor at Troy University's Computer Science Department, he holds a B.S. and M.S. in Electrical and Computer Engineering, and Ph.D. in EE and Statistics jointly. He conducts research in Cyber-Risk Informatics. He is the author of Trustworthy Computing (2007) and Cyber-Risk Informatics: Metric Evaluation (2014).

Preethi Vasudev is a part-time research associate at AUM and soon graduating from AUM's CSIS program with a Master's degree in August 2014. She holds a B.E. in Computer Science from Bangalore University, India. Preethi has worked in investment banking domain as senior consultant with Blackrock Inc. in London, England from 2008 to 2012.

Scott Morton is a part-time research associate at AUM and adjunct instructor at Troy University Montgomery campus. He holds a M.S. in Computer Science from Troy University Montgomery and a B.A. in International Relations from Johns Hopkins University.