INFORMATION SECURITY CULTURE IN THE BANKING SECTOR IN ETHIOPIA

Abiy Woretaw
Information Network Security Agency, Ethiopia
abiyworetaw@yahoo.com

Lemma Lessa
School of Information Sciences, Addis Ababa University
lemma.lessa@gmail.com

June 08, 2012

5th ICT 2012 Ethiopia Conference
Venue: UN ECA, Addis Ababa, Ethiopia

Outline

- Introduction
- Background Literature
- Research Motivation
- Research Objective
- Method
- Data Analysis
- Findings
- Conclusions and recommendations

Introduction

- The banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy.
- Banking business competition has stirred the advancement of services enabled by IT which in turn increased the information security risk.
- Information security encompasses technology, processes and people (Von Solms, 2000; Tessem and Skaraas, 2005).
- Although technical aspect of information security needs due attention, a more serious and under-rated aspect of information security is the human element.

Introduction (*Cont'd*)

- Many losses are not caused by lack of technology or faulty technology rather by users of technology and faulty human behavior.
- Martins and Eloff (2006) underline that the behavior of employees and their interaction with computer systems have a significant impact on the security of information.
- The purpose of information security culture is to address the various human factors that can affect an organization's overall information security efforts (Van Niekerk & Von Solms, 2005).

Information security culture (ISC)

- Martins and Eloff (2006) define information security culture as the assumption about acceptable information security behavior and it can be regarded as a set of information security characteristics such as confidentiality, integrity and availability of information.
- Information Security Culture is a subculture in regard to general corporate functions (Schlienger & Teufel, 2003).

Information security risks and threats in the banking sector

- Ula et al (2011) argue that information system has become the heart of modern banking in our world today.
- Any mishandling of confidential information asset can cause huge financial loss, and the reputation of the bank will be severely damaged.
- The Federal Deposit Insurance Corporation (FDIC) found Cyber thieves have cost US companies and their banks more than $15bn in the past five years.

Information security risks (*Cont'd*)

- Even big banks that generally do better job of security are found to be victims of security breaches.
- The New York giant bank, Citigroup reported a total of 360,083 North America Citi-branded credit cards were affected in the security breach that occurred in June 2011.
- Simply complying with the payment card industry digital security standards (PCIDSS) does not ensure credit card security.
- US Government is forcing banks to embrace risk-based security approach that incorporates all elements of the banks' information security.

Approaches and Requirements to promote organizational ISC

- Information security culture assessment approach consists of an audit process where the perceptions, attitudes, opinions and actions of employees regarding information security can be determined.
- Top management commitment, participation of employees, security awareness creation, allocation of budget, enhancing trust relationship and enforcement processes are among ways of promoting ISC.

Factors that influence information security culture and practices

- Organizational culture
- Top management support
- Information security risk analysis
- Information security policy
- Information security management standardization
- Information security awareness and training programs
- Information security compliance

Research Motivation

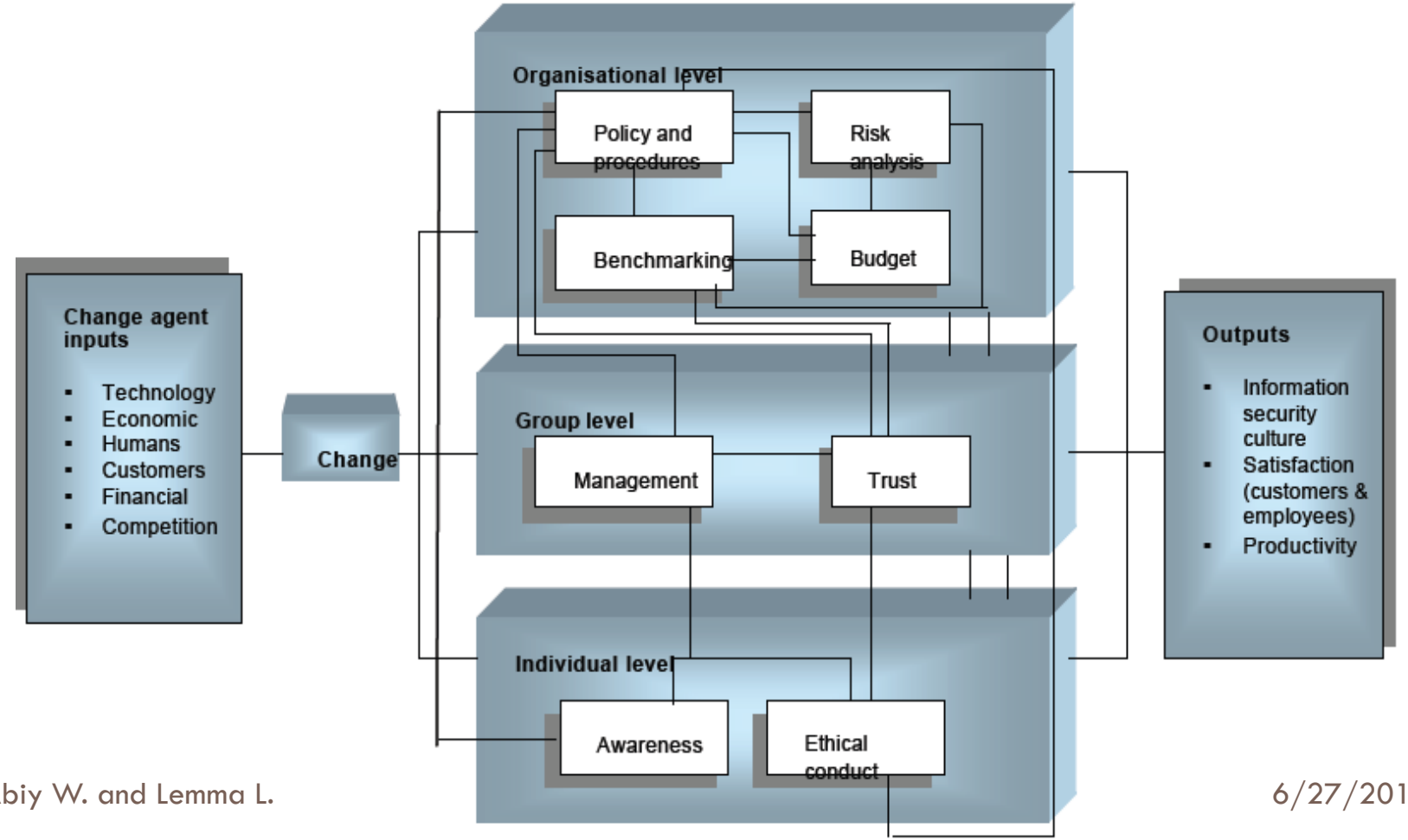
- A strong conviction in a research based approach to address information security challenges in Ethiopia.
- As financial institutions are more sensitive to security issues, priority is given to assess the level of information security culture in the banking sector in Ethiopia.
- In order to develop a successful information security culture within an organization, it is essential to understand the existing information security beliefs, practices and gaps.

Research Objective

- Assess the practiced information security culture in the banking sector in Ethiopia.
- Identify key gaps that need management and policy intervention so that effective information security culture can be established.
- Bridge the gap in researching the information security culture in the banking sector in Ethiopia.

Method

The research is based on a widely accepted information security culture model originally developed by (Martins, 2008).



Method (*Cont'd*)

- A survey research method is employed in order to assess the information security culture in the banking sector in Ethiopia.
- The level of information security culture in the banking sector in Ethiopia is evaluated by auditing process.
- A primary data is collected from headquarters of 11 different banks in Addis Ababa.
- A questionnaire to assess information security culture, developed by (Martins, 2008), is adopted.

Method (*Cont'd*)

- The ISC questionnaire has 41 statements designed to assess the knowledge, information security governance, communication, change management, performance management and trust level within an organization.
- Bank employees in the IT or Information Systems (IS) departments are the main participants of the survey.
- A non-probability convenience snowball sampling technique is used to collect data from all the banks.
- ISC data is collected from 4 governmental (37%) and 7 private (63%) banks.

Data Analysis

- 100 questionnaires were encoded into Statistical Package for the Social Sciences (SPSS) software for data analysis.
- The 41 ISC statements are categorized into the following six main ISC dimensions based on existing literature:
  - ***Knowledge and/or Perception dimension***
  - ***Information security governance and/or management dimension***
  - ***Communication dimension***
  - ***Performance management dimension***
  - ***Change management dimension***
  - ***Trust dimension***
- Binary Logistic Regression analysis is conducted to identify predictors of dependent variables.

Findings

- Only 31(31%) of the respondents are found to have adequate[>=50/55] information security awareness.
- Only 32(32%) of the collected data indicate that there is a proper information security governance [>=40/50] implemented in the banking sector in Ethiopia.
- Effective Communication [>=11/15] dimension indicated a slightly better score of 37(37%).

Findings (*Cont'd*)

- Promising trust relationship between employees and managers [>=20/25] in the banking sector is 35(35%).
- The level of readiness among employees to embrace information security changes [>=16/20] shows a slightly promising 38(38 %).
- Generally, the dimensional frequency analysis shows holistic and strategic work is needed to promote information security culture in the banking sector in Ethiopia.

Findings (*Cont'd*)

- Effective communication more likely affects the information security awareness development in the banks [AOR (95% CI) = 4.486(1.823, 11.040)].
- Effective communication is also observed to have created a positive trust environment[AOR (95% CI) = 4.594 (1.904, 11.084)].
- Positive trust relationship among employees and bank management seem to promote information security culture change[AOR (95% CI) = 3.481 (1.470, 8.245)].

N.B. [Adjusted Odds Ratio (95% CI) = the odds ratio(lower limit of the confidence interval, upper limit of the confidence interval)].

Findings (*Cont'd*)

- The prevalence of information security awareness to change management is also observed from the data analysis[AOR (95% CI) = 5.152 (2.071, 12.812)].
- Effective information security communication positively influences the readiness of employees to change their information security culture[AOR (95% CI) = 6.462 (2.629, 15.878)].
- The likelihood of proper information security governance establishment due to effective performance management is also observed [AOR (95% CI) = 6.821 (2.660, 17.486)].

N.B. [Adjusted Odds Ratio (95% CI) = the odds ratio(lower limit of the confidence interval, upper limit of the confidence interval)].

Conclusions

- Information security awareness in the banking sector in Ethiopia is unsatisfactory. Consequently, the level of proper information security governance in the banking sector in Ethiopia is a critical area of improvement.
- There is also a significant space to enhance the trust environment between managers and employees that can promote change in information security culture.
- The findings advocate the need for effective information security awareness, trust environment and communication to promote sustainable change in information security culture which enables proper information security governance and implementation that complies with local and international standards.

Recommendations

- Banks in Ethiopia should invest in effective information security communication methods like:
  - training employees with information security measures
  - information security awareness programs.
- International information security governance standards like ISO27002 and information security management standards like ISO27001 should be implemented at organizational level.
- More rigorous researches are needed to frame practical strategies to enhance the information security culture in the banking (and other) sectors in Ethiopia.

Thank You!