Cyber Security Risk Management Framework for Insurance Companies of Ethiopia

Etenesh Mulugeta
HiLCoE, Computer Science Programme, Ethiopia
eteneshmu@gmail.com

Mehari Misgana
HiLCoE, Ethiopia
m.g.msgna@gmail.com

Abstract

Risk appears in every kind of investment all over the world. Insurance companies are one of the investment/business sectors which are potential users of ICT infrastructure. Prioritizing where to focus resources to adequately protect the organization from cyber attacks is a challenge for many insurers. Insurance companies face many risks that present opportunities and challenges. Data disclosure, network security, cyber threats, and regulatory uncertainty are foremost on the list. This comes at a time when the industry continues to come with slower economic growth, high costs, low investment returns and market volatility.

The objective of this paper is to assess current Cyber Security Management (CSM) practices of the insurance sector and to propose and develop Cyber Security Risk Management (CSRM) Framework. In this work, attempt is made to examine and compare the available CSRM frameworks and best practices.

This research combines NAO (National Audit Office) cyber security and information risk guidance for Audit Committees checklist to assess the information systems security practices in the insurance industry. The results show that all surveyed insurance companies are found to be at low level of cyber risk management practice. The developed CSRM framework considers three key components, six dynamic interconnections which connect the three key components, and twelve security families. Addressing all of these three key components and six dynamic interconnections can lead to a holistic cyber security approach to cyber security risk management practices. For validation, five experts who have rich experience in the area of Information Technology and Information Security participated. The experts explained that the proposed framework is clearly constructed and easy to implement.

Keywords: Cyber Security Risk Management; Enterprise Risk Management; Business Model for Information Security; Dynamic Interconnection

1. Introduction

Insurance companies hold and process a vast amount of data including personally identifiable information, personal health information, credit card and bank account data, and trade secrets (their own and sometimes their clients'). To facilitate this activity, insurance companies use system which is done by Internet. They misuse such facilities by hacking insurance sites and cyber security threats could materialize due to lack of well-organized risk management framework. This is to mean that there is no cyber security risk management framework specifically prepared for the insurance sector in Ethiopia.

The majority of the research about CSRM has been performed by technologically leading countries. On top of this, major information security international standards are written from a Western perspective, without knowing how applicable CSRM concepts and practices are to other cultures, which have different social, organizational, and security cultures [3].

Various studies in Ethiopia have addressed different aspects of CSRM framework customization in the banking sector. These include works by Eshetu Burisa [1], Kelemie Tebkew Yirdaw [2], and Meskerem Alemu and Abrehet Mohammed Omer [4]. There is a need for CSRM framework design in the insurance sector. The reason is that the legal, audit, compliance, privacy, business continuity, quality control, facilities, human resources, IT security, information security, and physical security are different from the banking industry and from other countries' contexts.

Ethiopian insurance companies have challenges due to lack of well-organized risk management framework. For such companies, it is difficult to

- manage risk as business transforms,
- understand the broader risks of new technologies,
- provide digital trust and privacy, and
- monitor cyber security risk management activities at national level.

Our framework enables insurance companies to overcome those problems. It defines the essential components and procedures of a systematic cyber security risk management. By following our framework, they can easily manage risks to ensure the confidentiality, integrity, and availability of their information systems.

The following research questions are formulated.

- How are the existing international cyber security risk management frameworks suitable for Ethiopian insurance sector?
- What is the existing cyber security risk management status of Ethiopian insurance sector?
- What are the key issues and influencing factors that surround the effectiveness of cyber security practice in the insurance sector of Ethiopia?
- What cyber security risk management framework should be developed to meet the challenges of today's cyber threat landscape for the Ethiopian insurance sector?

Both qualitative and quantitative research approaches were used and data were collected via questionnaire and interview. To analyze the data cross case data analysis and Likert scale data analysis tools are used.

The framework provides the following advantages to Ethiopian insurance companies:

- A common language to address and manage cyber security risk,
- Minimizes the risk of attacks,
- Increases knowledge of competence in relation to cyber security,
- Benchmarking the organization in relation to peers in the field of cyber security,
- Better information on cyber-crime trends and incidents to facilitate decision making, to address identified risks and minimize the impact of compromise,
- Clearer communication on the theme of cyber security, enabling everyone to know his/her responsibilities and what needs to be done when an incident occurs or is suspected, and
- Improved reputation, as an organization that is well prepared and has given careful consideration to its cyber security is better placed to reassure its stakeholders.

2. Related Work

A cyber risk management framework is developed based on NIST's Cyber Security Framework and expands it by adding a cyber-maturity evaluation [5]. It defines board engagement and oversight based on six security families. These are legal and compliance, leadership, technology, human factor, business continuity and information risk management. The framework is high level and difficult to implement but it shows what things are incorporated when a board participates on each of the above six security families.

The work in [6] includes core risk culture, risk organization, and risk governance. It recognizes the external impacts and influences of the economy, marketplace, and views of regulators, investment community and rating agencies. A successful ERM framework provides an integrated and iterative approach with a commitment to continuous improvement. These are identification, evaluation, mitigation strategy, and monitoring results.

The work in [7] focused on how insurers manage physical and digital assets to protect brand and reputation. The focus areas are operating model and culture, process and assets, roles within the organization and investment in proactive security. It emphasizes the importance that insurance companies are placing on creating a secure and common infrastructure for the digital economy. It highlights the need for resilience and attribution to secure the integrity and intimacy chain between client and

insurer. The work used this to define information security risk management family.

NIST Special Publication 800-39 suggests effective management of risk for information systems using six iterative steps [8]. These are categorize information system, select security controls, implement security controls, assess security controls, authorize information system, and monitor security controls

This framework is generic to manage information risk and the researchers used this to define information risk management security family from insurance perspective.

ISO 31000:2009 focused to assist an organization to integrate risk management within its overall management system using five iterative steps [10]. These are context establishment, risk identification, risk analysis, risk evaluation, and risk treatment.

The work in [9] focused on handling of information and cyber security related issues based on 16 security families. It is essential to ensure that a uniform framework for information and cyber security is implemented across the insurance industry and an in-built governance mechanism is in place within the regulated entities in order to make sure that all such security related issues are addressed from time to time. IRDAI framework is used to define the security families as much as necessary from the Ethiopian insurance sector perspective.

3. Survey Result and Discussion

The research findings are classified into two major areas, finding from questionnaire and finding from interview. Finding from questionnaire provides how cyber security risk is managed in the surveyed insurance sectors. Finding from the interview clarifies the general issues in cyber security risk management framework implementation.

i. Questionnaire Analysis

All controls which are found in questionnaires are summarized in Table.

Table 1: Summary of Security Control

No.	*Control Family*	*Risk Category*	*Status*	*Status*
1.	Access Control Family	Process	Medium	Medium
2.	Awareness and Training Family	People	Low	Low
3.	Audit and Accountability (AU) family	Technology	Low	Low
4.	Identification and Authentication Family	Technology	Medium	Medium
5.	Risk Assessment Family	Process	Low	Low
6.	Maintenance family	Process	Medium	Medium
7.	System and Information Integrity Family	Process	Low	Low
8.	Physical Protection Family	Process	Medium	Medium
9.	Incident Response Family	Process	Low	Low

ii. Interview -Analysis

a. Availability of Cyber Security Risk Management Organizational Unit

All surveyed insurance companies had no cyber security risk management unit. But all insurance companies have risk management department but no IT professionals. Because of this the risk management department accesses finical risk only. Therefore, managing cyber risks, assessing cyber risks, mitigating cyber risks and other related issues under cyber risk are the responsibility of information security unit. Critical Mass Cyber Security Requirement standard recommends organizations to have cyber security risk management unit. Based on this, the insurance sector planned to have cyber security risk management unit which is responsible for only managing cyber security risks.

b. Developing Risk Assessment Strategy and Assessing Cyber Security Risk

Risk assessment is the process of identifying threats and assessing the likelihood of those threats exploiting some organizational vulnerability, as well as the potential impact of such an event occurring [5]. From surveyed insurance sectors most insurance companies cannot access risk in regular way. This indicates that insurance sector does not give attention for risk assessment.

c. CSRM Frameworks and Guidelines

All surveyed insurance companies do not use cyber security risk management framework. There are different challenges that delayed the designing and implementing of insurance wide CSRM. Some of them are lack of: CSRM understanding by top management, employee motivation, budget due top management low attention, and domain experts.

d. Challenges of Insurance to Secure their Cyber Profile

Generally all Ethiopian insurance companies have fully or partially the following problems.

- Lack of knowledge about cyber security risk: there is no training on cyber risks. Besides, employers, including IT staff, assume that there is no cyber risk in the insurance sector.
- The dynamism of technology: information technology by nature changes from time to time and it is resource intensive to evolve more radically to defend against new competitors and continue to grow business.
- Infrastructure: this one of the major challenges that insurance companies face.
- Telecom: since there is only one Internet subscriber in the country, it is a challenge to provide effective service to consumers.
- There is no local CSRM Framework or guidance in the insurance companies.
- Work overlap in IT department: one IT professional assigned to multiple tasks.
- Attention for security is not given by top management.
- There is no investment for a long period on security.
- No well-organized security team for monitoring security status of each system and network within its control.

e. Insurance Recommendation

The following are recommend in order to make cyber security risk management standards, frameworks and guidelines suitable for Ethiopian insurance companies:

- Identify the objective of the organization.
- Make the frameworks sector and industry specific.
- Professionals shall participate in the development of the framework.
- Each stakeholder should participate on the development of the framework.
- It is better to understand the insurance business before developing the framework. For example, identify the core processes and core customer facing application.
- Differentiate critical business applications.
- Understand transaction applications.
- Understand the external and internal drivers.
- Conduct research and gather enough data about main risks.
- Develop the culture of managing cyber risks.

4. The Proposed Solution

The framework is proposed based on the BMIS model in [7] and applying necessary customization on components of the model that are useful for insurance companies and formulate related security families and activities under each component. We considered three key components and six dynamic interconnections which connect the three key components as shown Figure 1 to propose the CSRM framework. This provides a comprehensive and in-depth view of an organization's cyber security risk management practice. Addressing all of these three key component and six dynamic interconnections can lead to a holistic cyber security approach to cyber security risk management practices.

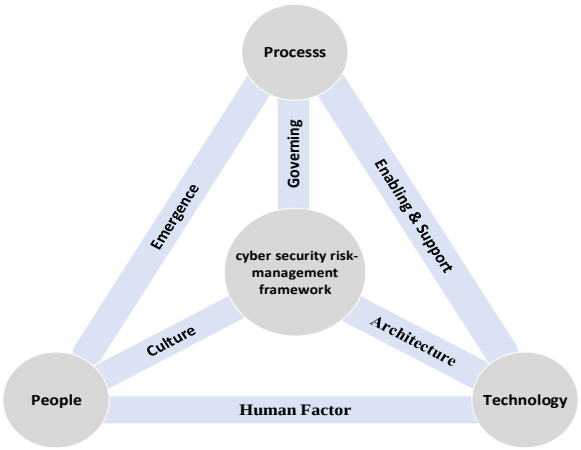

Figure 1: The Proposed CSRM Framework

4.1 Components of the Proposed Framework

The proposed framework has the following components.

1. Process

It derives from the strategy and implements the operational part of the organization element [7]. We used the following three security families to define the process part of the framework.

a. Access Control

Access control should address the following issues from insurance cyber security perspective [12].

- Access control mechanisms should restrict the business application that enables access only to the particular capabilities needed to fulfil a *defined role*.
- Additional controls should be applied to special access privileges, including high level privileges, e.g., *root* in Unix or *Administrator* in Windows operating systems.
- All 'Users' shall be authenticated at a minimum by using User IDs and passwords, before they can gain access to target systems.
- Repository for all users including third parties should be maintained.

b. Information Risk Management

We defined four iterative and cyclic processes for assessing and mitigating information risks as shown in Figure 2.

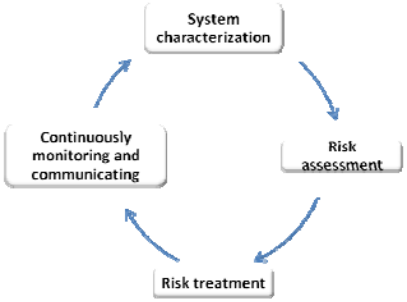

Figure 2: Iterative and Cyclic Processes

c. Business Continuity (BC)

The risk management should address the following ideas regarding business continuity.

- The organization shall have BC policy
- The BC policy has to be communicated
- Business impact analysis shall be conducted
- Develop Emergency response plan
- Validate the on-going effectiveness of its BC planning
- Review the Organization's BC preparedness

2. People

It represents the human resources and the security issues surround them. We considered two security families to define the people component.

a. Staff of the Cyber Security Team

The roles and responsibilities of cyber security team in an insurance company are defined as follows [7].

- *Chief Executive Officer (CEO)*: include cyber security in management strategy and goals.
- *Chief Information Security Officer (CISO):* develop cyber security strategy and monitoring program.
- *Chief Compliance Officer (CCO):* comply with laws and enforce policies and regulations.
- *Chief Security Officer (CSO):* focus on business continuity and planning.
- *Chief Risk Officer (CRO):* build cyber security into enterprise risk framework.
- *Chief Information Officer (CIO):* enhance cyber security posture within existing technologies.
- *Chief Market Officer (CMO)*: respond rapidly to media and public relations issues.
- *Chief Operations Officer (COO):* embed cyber security awareness culture into operation.

- *Chief Financial Officer (CFO):* monitor financial anomalies and evaluate insurance claims
- *Chief Human Capital Officer (CHCO)*: optimize cyber security talent.

b. Legal and Compliance

Government and regulatory bodies are driving cyber-related governance practices around the collection, storage and use of data. It includes:

- Develop clear business aligned program for information security,
- Assign responsibilities, and
- Support the IS Policy by providing sponsorship and budget.

3. Technology

The technology component of the framework is composed of all of the tools, applications and infrastructure that make processes more efficient. It includes:

a. Effective User Group Management: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization.

b. Network Access Control: Filter out unauthorized access and malicious content.

c. Application Security: consider the following points [9]:

- Each application shall have an owner,
- Information security requirements analysis and specification,
- Technical review of applications after operating platform changes, and
- Secure development environment.

4.2 Dynamic Interconnections (DIs) of the Proposed Framework

1. *Governing*: The Governing DI represents the steering of the enterprise and demands strategic leadership. It includes
   - Information Security Policy
   - Leadership and Governance
   - Strategic leadership
2. *Culture*: the culture DI represents a pattern of behaviours, beliefs, assumptions, attitudes and ways of doing things. It considers putting the right people, skill and knowledge in the right place.
3. *Architecture*: to build the insurance company's security architecture, enterprise security is better than the other.
4. *Enabling and support*: it ensures that people comply with technical security measures, policies and procedures to make processes usable and easy [11]. It includes:
   a. *Change Management:* Changes to business applications, computer systems and networks shall follow a change management process covering associated risks, change authorization, business continuity and impact.
   b. *Vendor/Third party Risk Management*: The risks to the organization's information and related information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented.
5. *Emergence*: it is the consideration of emergent issues in system design life cycle, change control and risk management [11]. It includes:
   - Response and Recovery contingency plan
   - Incident Reporting & Escalation handling Processes & Procedures
   - Review of the functioning of the preventive and detective controls
6. *Human factors:* it represents the interaction and gap between technology and people. It includes:
   - Information Security Awareness
   - Information Security Training

5. Discussion

It is found that the existing international risk management standards, frameworks, guidelines and models are not suitable because the standards are too generic and most of them are not industry specific.

Findings of the assessment based on the fact finding techniques employed, such as questionnaire survey and interviews, show that current cyber security risk management status in the surveyed insurance companies generally lack a formalized and comprehensive framework-based approach. This

seemed to have an adverse effect on the effective management of cyber security in insurance companies.

The key issues and influencing factors that surround the effectiveness of cyber security practice in insurance companies are the risk of loss resulting from inadequate or failed internal processes, people and technology. Security managers face myriad challenges, including changing risk profiles, lack of funding, cultural issues, and internal and external threats.

Developing a cyber security program and integrating it into business goals, objectives, strategies and activities is complicated by the lack of a framework that describes what an effective cyber security program encompasses, how it functions, and how it relates to the organization and the organization's cyber security priorities.

The framework will benefit a range of stakeholders by reducing costs, improving performance, fostering a better understanding of organizational risks, increasing collaboration and reducing duplication of effort. Diligent utilization of the framework will equip insurances to deal with current and future issues such as: regulatory requirement, globalization, growth, scalability, organizational cooperation, evolving technology, economic markets, human resources, competition, ever-changing threats, and innovation.

The developed CSRM Framework can be used as a starting point for the insurance sector to manage cyber security by developing guidelines and implementing controls to protect assets from cyber attacks.

6. Conclusion and Future Works

The framework developed in this paper is an integration of all available framework components discussed and derived from literature review and findings of questionnaire and interview. The framework for cyber security presents a systemic view of how a cyber security program operates. It captures the dynamic interconnections - the forces that exert the greatest influence on cyber security programs - and to a great extent, determine the ability of programs to achieve their goals. The framework can be used to predict how a change in technology, process and human resources is impacted by culture, human factors or the other dynamic interconnections.

Some aspects of CSRM that are not considered and will be investigated in the future include the following:

- Determining the impact level of trust, ethical conduct, and culture on the process of CSRM development and implementation.
- Evaluating the proposed CSRM framework practically via comprehensive test in the real insurance environment.

References

[1] Eshetu Burisa, "Information Security Risk Management Framework in Ethiopia: The case of Commercial Banks", 2016.

[2] Kelemie Tebkew Yirdaw, "Information Security Management Framework for Banking Industry in Ethiopia", June, 2013.

[3] Mohammed, A., and Karen, N., "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context", in Proceedings of the 7th Australian Information Security Management Conference, 2009.

[4] Meskerem Alemu and Abrehet Mohammed Omer. "Cloud Computing Security Framework for Banking Industry", 2014.

[5] Andrea Zapparoli Manzoni, "Cyber Risk Management from the CSIRT to the Board and Back", Enabling Business Security, May 2016.

[6] ERM Committee of the American Academy of Actuaries. "Insurance Enterprise Risk Management Practices." March 2013, https://www.actuary.org/files/ERM_practice_note_030713_exposure.pdf, Last accessed on Sep 27, 2018

[7] EY, "Cyber strategy for Insurers", 2017, https://www.ey.com/Publication/vwLUAssets/ey-cyber-strategy-for-insurers/$File/ey-cyber-strategy-for-insurers.pdf, Last accessed on Sep 20, 2018.

[8] Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, and Gary Stoneburner, "Managing Risk from Information Systems",

NIST Special Publication 800-39,2001, pp. 5-20.

[9] Insurance Regulatory and Development Authority. “Information and Cyber Security Framework for Insurance Sector”, India, October, 2016, https://nios.ac.in/media/documents/VocIns Services/m5-f2.pdf, Last accessed on Oct 28, 2018.

[10] ISO/IEC27005, “Information Technology Security Techniques for Information Security Risk Management.” 2011, http://www.accelerosblog.com/wp-content/uploads/2011/05/INCITS+ISO+IEC+27001-2005.pdf, Last accessed on July 29, 2018.

[11] ISAC, “An Introduction to the Business Model for Information Security.” 2009, http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf, Last accessed on Sep 27, 2018.

[12] Gary Stoneburner, Alice Goguen, and Alexis Feringa, “Risk Management Guide for Information Technology Systems.” 2002, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf, Last accessed on Oct 13, 2018.