International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17 (2017) pp. 6983-6987


# Cyber Security Insurance Status in Malawi

**Kondwani Makanda*, and Hyunsung Kim****

**Computer Science Department, Malawi University of Science and Technology, Malawi.*
*Department of Cyber Security, Kyungil University, Korea.*

***Corresponding Author*

**Orcid ID: 0000-0001-6132-316X , **Orcid ID: 0000-0002-7814-7454*

**Abstract**

This paper is to show the status of cyber security insurance (CSI) market in Malawi. For this, we did research to find out whether insurance companies in Malawi provide CSI to mitigate the negative effects of cyber-attacks or data breaches. Based on our research we find out that the concept of CSI in new in Malawian context and also we did not find detailed literature concerning CSI in Malawi hence making this research novel. Seven general insurance companies were contacted to find out if they do provide CSI and if they do (representing all general insurance companies on the Malawian market) what kind of policies are involved. To our surprise we found out that no insurance company in Malawi does provide CSI policies. This can be an advantage because Malawi can learn from more mature countries and avoid mistakes that were made when they were developing CSI industry. This can also act as a disadvantage because companies will not be able to transfer risk once cyber breach happens.

## INTRODUCTION

Cyber security is a major concern for any country. This is due to the rise in dependency of computers and computing devices that are connected to the Internet [1]. Sectors such as banking, health, energy, transport and drinking water supply and distribution are some of the critical sectors where cyber security insurance (CSI) can play a vital role [2]. For companies, organizations and even countries to mitigate the negative impact that can arise from of cyber security risks, CSI can be used as one option of transferring risk where CSI will involve the transfer of risk, risk mitigation and risk response or recovery [3].

In general, computer security falls under three main objectives shown in Fig. 1 where all the three objectives, confidentiality, integrity and availability, have to be maintained. Confidentiality prevents unauthorized access to information, integrity makes sure that the accuracy and consistency of data and systems are maintained and assured and lastly availability makes sure that computer system, data and communication channels are not denied to authorized users [4-5].

Although CSI had a low adoption rate even in some highly industrialized countries, governments like the British is supporting the growth of CSI to act as the way of managing cyber security risk [2, 6]. The low adoption of CSI can be attributed to low awareness of cyber security threats organizations have as depicted in Fig. 2.

CSI can cover the following aspects [3, 6]

- Costs for forensic investigations and customer notification
- Costs of system restoration
- Costs of fines and coverage in relation to cyber breaches
- Data privacy coverage
- Legal costs of cyber breaches
- Media or public relations costs of cyber breaches
- Lost revenue resulting in business interruptions
- Cost of cyber extortions.

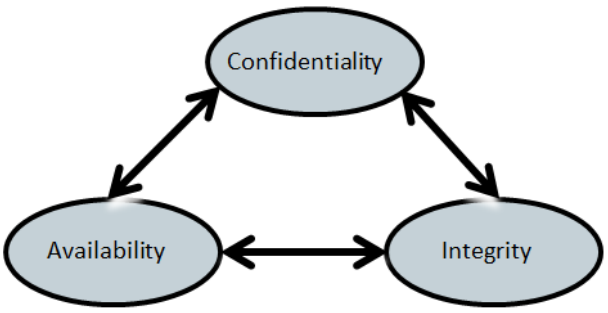


**Figure 1:** Confidentiality, integrity and availability triad [4-5].

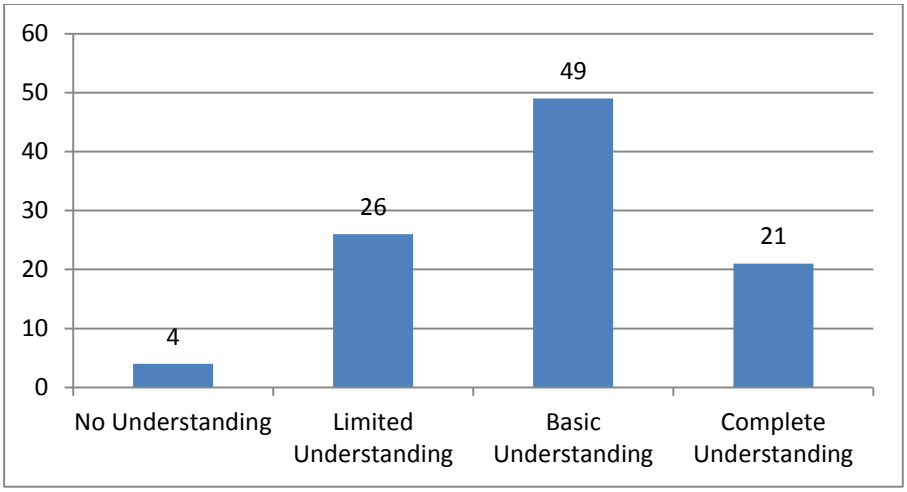


**Figure 2:** Cyber risk understanding of organizations in Europe [2].

This research is focused on whether CSI is provided by the 7 insurance companies that are active on the Malawian market. It is based on the work done by [6] due to a number of reasons one of them being that [6] did research in a more matured CSI market, highly advanced and connected country of Sweden.

The main question asked in this paper is that: Is there any CSI provider in Malawi? If so, how is the insurance provision like? Based on these points, we decided to conduct research on the CSI on the Malawian market.

The rest of the paper is organized as follows: in Section II, we provide a brief description of the general insurance industry in Malawi, in Section III we provide related works, in Section IV we discuss the methodology and results used in conducting our research. In Section V we provide our recommendations and lastly in Section VI we provide the conclusion.

## INSURANCE IN MALAWI

Malawi as one of the least developed countries has an insurance industry that has been in existence for more than 60 years with low Internet penetration [7-8]. Currently the insurance industry is supervised and regulated by the Reserve Bank of Malawi [12]. Malawi has seven licensed general insurance companies [9-10]. The Insurance Institute of Malawi is there to provide the insurance industry with education and training of insurance professionals [11]. As stated its main objective is to advance professionalism and its mission is to act as a center of excellence for insurance and financial services, knowledge and professionalism [11].

The threats of cyber security breaches and attacks have not spared Malawi. This is because Malawi is increasingly becoming reliant on the Internet and computer networks in conducting business [1]. Malawi as a developing country is not spared of this concern. As [6] pointed out, not all computer security threats, computer breaches and unavailability of information technology (IT) systems can be solved or prevented through information and communication technology (ICT) technical solutions. CSI can be used as one way of handling these threats.

Malawi government, private companies and nongovernmental organizations are moving in cyber space as a way of delivering service to the citizenry. E-commerce is one of the fastest growing and most thriving industries in Malawi due to the use of mobile devices [7]. Activities like money transfers, payment of utility bills and commodity exchange are being conducted using mobile devices. There is little insurance in the ICT industry although vandalism is one of the negatives effects that the ICT sector suffers. This makes the need for CSI to be a way that these companies can help to handle cyber security threats and transfer the risk.

## RELATED WORK

Cyber risk which is the risk associated with the use of electronic data and how the data is being transmitted and also involves the use of Internet and telecommunication network [3]. These cyber risks which can be both internal and external can result in costs worth millions to organizations [3-4]. In the United States of America (USA) alone, the CSI market has reached $2 billion and is estimated to reach $7.5 billion additionally this is projected to grow in both USA and Europe [2-3].

Government regulation has also been found to have an impact on the rise in adoption of CSI [2]. These regulations could include citizen's right to know when there is a cyber security breach in an organization, fines being introduced and mandatory notification by organizations affected by cyber breaches [2].

In [3], three reasons were provided as to why and organization may choose CSI. The reasons include

- Monetary value on the organizations' cyber risks – this helps an organization in security risk

budgets with senior management who are mostly not aware or well appreciative of the importance of cyber security threat and the money needed to mitigate and prevent such incidents from happening.

- CSI can help organizations in identifying cyber security shortcomings or gaps – this can help an organization in finding ways of improving cyber security weaknesses.
- CSI can help organizations in risk transfer, risk mitigation and also incident response.

Provision of CSI can also act as an incentive to encourage customers to invest in cyber security since insurance companies will not insure them if they cannot meet a minimum cyber security threshold required by the insurer [2, 6].

On the insurer's part, challenges such as the unavailability of data related to cyber security incidents in support of risk assessment which would support risk assessment of the customer [2]. Other reasons include, lack of awareness by the customers in the availability of CSI, lack of technical expertise, customer's lack of willingness in sharing documentation regarding cyber security incidents, lack of understanding of new threats and how to detect them and the calculation of cost on the basis of the cyber security incident [2][ 4].

## METHODOLOGY WITH RESULTS

In this research we wanted to find out whether CSI is like in Malawi. For us to do this we conducted a survey of the seven registered companies which are: Charter Insurance Company Ltd, General Alliance Insurance Company Ltd, NICO General Insurance Company Ltd, Prime Insurance Company Ltd, Britam (REAL) Insurance Company Ltd, Reunion Insurance Company Ltd and United General Insurance Company Ltd. One-to-one interview questions were asked to the representatives of all the seven companies. Open discussion was also used as a mean of getting data from these representatives. A number of questions were crafted to be used in our research but based on the results that we were getting. Most of these questions were not asked.

In our research the first question that was asked was to find out whether CSI is provided by the companies or not. Based on that question the following results shown in Table 1 were found.

**Table 1:** Results of whether CSI is provided or not.

| Code | Insurance Company | Do you provide CSI? | |
|---|---|---|---|
| | | Yes | No |
| IC1 | Charter Insurance Company Ltd | | ✓ |
| IC2 | General Alliance Insurance Company Ltd | | ✓ |
| IC3 | NICO General Insurance Company Ltd | | ✓ |
| IC4 | Prime Insurance Company Ltd | | ✓ |
| IC5 | Britam (formerly REAL) Insurance Company Ltd | | ✓ |
| IC6 | Reunion Insurance Company Ltd | | ✓ |
| IC7 | United General Insurance Company Ltd | | ✓ |

**Table 2:** Results of whether the companies do intend to introduce CSI in the near future.

| Code | Insurance Company | Do you intend to introduce CSI in the near future? |
|---|---|---|
| IC1 | Charter Insurance Company Ltd | Maybe (Soon after October) |
| IC2 | General Alliance Insurance Company Ltd | May not |
| IC3 | NICO General Insurance Company Ltd | Maybe |
| IC4 | Prime Insurance Company Ltd | Not sure |
| IC5 | Britam (formerly REAL) Insurance Company Ltd | Not yet |
| IC6 | Reunion Insurance Company Ltd | Maybe depending on demand |
| IC7 | United General Insurance Company Ltd | May do so |

Based on the fact that all insurance service providers do not provide CSI, the next question that was asked was to find out whether or not they intend to introduce it the near future. The results for this question are shown in the Table 2. The other question that was asked was about introduction of cyber security policy in the near future.

During our discussions some important points were mentioned including the following: IC7 mentioned that it will be difficult to calculate charges in order to come up with the right premiums. IC7 also mentioned that government regulations and technology affects their market they also said they can insure laptop in case of theft or loss. IC6 also mentioned a number of issues that can affect the roll out of this product such as that most products that are being offered are tradition products here where CSI is not one of them. Lack of innovation, low levels of disposable income and lack of target market for CSI were also mentioned as another factor that can affect CSI policies by IC6.

## RECOMMENDATIONS

Based on our research we have found that there is no insurance company in Malawi that offers CSI policy. The other thing is that most of these insurance companies do not envision starting to provide CSI policy anytime soon. We recommend that when insurance companies start offering CSI services, they should implement some of the methods that [6] highlighted i.e. the insurance companies should demand high standards if any company is supposed to be covered and reject all organizations that have poor cyber security policies. From the research conducted it is imperative that the government or the industry itself should devise insurance mechanisms to cover cyber security incidents.

Based on our study we feel that if CSI is adopted in Malawi, a number of benefits can occur including some of the following

- We believe that by providing CSI can encourage large multinational companies or organization to set businesses in Malawi since they will know that their ICT infrastructure is insured.
- The insurance can act as a catalyst for best practice in cyber security. This is so because insurance companies will only cover companies or organizations that have met the minimum standards required in cyber security.

We also feel that if some of the products that are provided in other developed countries it will really help Malawi. Some of the products that can be incorporated in the Malawian context as is done in [6] can include

- Loss of revenue as a result of business interruption which can include costs due to security attacks, system failures not due to security attacks
- Cost of doing forensic investigation as a result of an attack
- Cost of cyber extortion
- Cost of public relations to cover reputation damage due to cyber-attack or data breach
- Cost of legal and regulatory fees
- Cost of system restoration
- Cost of data and privacy breaches
- Spread of malware that is spread from the insured organization's computer systems

However, it is necessary to adopt those products in step-by-step-wise not at once. Thereby, we also need to develop a reasonable priority list to plan the products by considering and depending on each country's ICT status.

## CONCLUSION

From the research that we conducted, it shows that currently there is no CSI provider in Malawi. This can have a negative impact on the overall information or cyber security in Malawi since some companies that work with sensitive data will not be willing to invest in Malawi due to lack of CSI. Based on our discussion, it has been shown that CSI can help to improve cyber security of nations or companies since the insurance companies will not be willing to insure organizations that does not implement required minimum cyber security measures.

## ACKNOWLEDGEMENT

Corresponding author is Hyunsung Kim. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

## REFERENCES

[1] Malawi Communication Regulatory Authority, *Strategic Plan 2015-2020*, http://www.macra.org.mw.

[2] European Union Agency For Network and Information Security, *Cyber Insurance: Recent Advances, Good Practices and Challenges*, 2016, www.enisa.europa.eu, doi: 10.2824/065381.

[3] American Bankers Association, *2016 Cyber Insurance Buying Guide*, 2016, https://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf.

[4] Ernst & Young LLP, *Cyber Insurance, Security and Data Integrity: Part 1: Insights into cyber security and risk — 2014*, 2014, http://www.ey.com/insurance.

[5] W. Stalling, *Cryptography And Network Security Principles And Practice,* 5th Edition (2011), Pearson Education, Inc., New York, USA.

[6] U. Franke, "*The cyber insurance market in Sweden*,"

Computers & Security, Vol. 68, pp. 130-144, 2017, http://dx.doi.org/10.1016/j.cose.2017.04.010.

[7] B. Kampanje, "*PESTEL analysis of Malawi's non-life insurance industry*," African Journal of Economic and Management Studies, Vol. 5 No. 1, 2014, https://doi.org/10.1108/AJEMS-01-2013-0002.

[8] International Telecommunication Union, *Cyberwellness Profile Malawi*, www.itu.int/en/ITU-D/Cybersecurity/ Documents/Country_Profiles/Malawi.pdf.

[9] https://www.rbm.mw/Home/GetContentFile/?ContentID=7697.

[10] http://www.insuranceassociationmalawi.com.

[11] The Insurance Institute of Malawi, http://www.iim.org.mw/.

[12] https://www.rbm.mw/Supervision/PensionsandInsurance/?activeTab=PISUAbout.