TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Tornike Nanobashvili 156337IVCM

IMPROVING THE USE OF A CYBER-INSURANCE PRODUCT IN GEORGIA: THE EXAMPLE OF COMMERCIAL BANKS

Master's thesis

Supervisor: Eneken Tikk
PhD
Co-Supervisor: Mika Juha Kerttunen
PhD

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Tornike Nanobashvili 156337IVCM

KÜBERKINDLUSTUSE KASUTAMISE EDENDAMINE GRUUSIAS KOMMERTSPANKADE NÄITEL

Magistritöö

Juhendaja: Eneken Tikk
PhD
Kaasjuhendaja: Mika Juha Kerttunen
PhD

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Tornike Nanobashvili

10.02.2019

Abstract

This master's thesis contributes to promoting cyber-insurance in the Republic of Georgia. An empirical study conducted via semi-structured interviews with insurance companies and commercial banks indicates that cyber-insurance has not become widely offered and used in the Georgian market.

Based on interviews with insurance companies, the study develops a deeper understanding of the reasons for the low supply of cyber-insurance product. The research further investigates reasons for modest demand for cyber-insurance by commercial banks, one of the most vital sectors in the Georgian economy and business exposed to significant cyber threats.

The thesis concludes with recommendations on promoting and further developing cyber-insurance products in Georgia. Findings of the study can be implemented to evolve cyber-insurance portfolios and integrate cyber-insurance products in cyber risk management strategies of commercial banks. Therefore, the master's thesis makes the contribution to cyber-insurance and cyber risk transfer research as well as to Georgian cybersecurity.

This thesis is written in English and is 82 pages long, including 3 chapters, 8 figures and 4 tables.

Annotatsioon

KÜBERKINDLUSTUSE KASUTAMISE EDENDAMINE GRUUSIAS KOMMERTSPANKADE NÄITEL

Käesoleva magistritöö eesmärk on aidata kaasa küberkindlustuse edendamisele Gruusias. Kindlustusettevõtete ja kommertspankadega tehtud poolstruktureeritud intervjuudel põhinenud empiirilisest uuringust nähtus, et küberkindlustust ei pakuta ega kasutata Gruusia turul suurel määral.

Kindlustusettevõtetega tehtud intervjuude alusel annab uuring põhjaliku ülevaate küberkindlustuse vähese pakkumise põhjustest. Samuti keskendutakse uuringus põhjustele, miks kommertspankade nõudlus küberkindlustuse järele on tagasihoidlik, arvestades, et tegemist on Gruusia ühe olulisima majandussektoriga, kus küberohtude risk on suur.

Magistritöö kokkuvõttes esitatakse soovitused küberkindlustuse edendamiseks ja täiustamiseks. Uuringu tulemusi on võimalik kasutada küberkindlustusportfellide arendamiseks ning küberkindlustuse integreerimiseks kommertspankade küberriskide juhtimise strateegiatesse. Seda arvesse võttes annab magistritöö panuse küberkindlustuse edendamisse, küberriskide ülekandmist käsitlevatesse teadusuuringutesse ning laiemalt ka küberturvalisuse tagamisse Gruusias.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 82 leheküljel, 3 peatükki, 8 joonist, 4 tabelit.

Acknowledgements

I want to express my special thanks and gratitude to my supervisors: Dr Eneken Tikk and Dr Mika Juha Kerttunen, for their lectures, support and recommendations to accomplish the master's thesis.

I am very grateful to the Tallinn University of Technology and the University of Tartu with all the lecturers giving me the possibility to enlarge my knowledge and improve my skills. I appreciate a lot being granted to study free of charge and being the scholarship member of such wonderful universities.

My deepest and profound gratitude to my parents for their love, support and encouragement that teach me to be a human and motivate never to give up but strive for the best.

Many thanks to my second home Estonia in opening doors to the new level of opportunities and challenges.

Finally, I am thankful to all the respondents, who contributed to the research and dedicated their time to give out the feedback.

List of abbreviations and terms

CGL	Commercial general liability
CIA Triad	Confidentiality, integrity and availability
CSI	Computer security institute
ENISA	The European Union Agency for Network and Information Security
EU	European Union
FBI	Federal Bureau of Investigation
GDP	Gross domestic product
GDPR	General data protection regulation
ICT	Information and communication technologies
IDS	Intrusion detection system
IC3	Internet Crime Complaint Center
IoT	Internet of things
ISIC	International student identity card
IT	Information technology
LEPL	Legal Entity of Public Law
NBG	National Bank of Georgia
OECD	Organization for Economic Cooperation and Development
PR	Public relations
P&C	Property and casualty
TUT	Tallinn University of Technology
USA	United States of America

Table of contents

List of figures

List of tables

INTRODUCTION

The rapid development of information technology (IT) in the 21st century has made a significant impact on the way people live, get information and deal with everyday challenges. As the IT industry continues to develop, companies are moving from traditional paper-based solutions into the information systems, since it offers many flexible business opportunities and reduces cost, increases operation's time efficiency, etc. However, using internet and information systems, also open doors to the new level of risks and concerns.

In the 21st high-tech century, cybercrime has become an everyday matter of life, where the returns are high, and the risks are low. "Internet Crime Complaint Center"'s[1] (IC3) report within 2014-2018 years range in the United States of America (USA) shows,[2] that there are total 1,509,679 complaints of internet crime with the losses of 7.45 billion dollars, which is 7.93 percentage to the gross domestic product (GDP) of USA for the same time interval.[3] In other words, the smallest of cybercrime figures are more than some of the nation's GDP.[4] The IC3's report indicates that the cybercrime increases annually, but companies still underestimate cyber threats and cyber risks quickly increase.

Important to outline, that throughout this master's thesis cybercrime and cyber-attacks are used interchangeably only within the cyber-insurance context and exclude the type of cyber threats that are connected to cyber warfare and cyber terrorism. Also, financial institutions that unite wide range of financial service providers are referred with the same meaning as the commercial banks and used interchangeable.

---

[1] Federal Bureau of Investigation Internet Crime Complaint Center (IC3). Available at: https://www.ic3.gov/about/default.aspx [Accessed: 07.05.2019]

[2] 2018 INTERNET CRIME REPORT. Available at: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf [Accessed: 07.05.2019]

[3] The percentage calculation of the losses to the total gross domestic product within 2014-2018 interval has done by me. United States GDP. Available at: https://tradingeconomics.com/united-states/gdp [Accessed: 07.05.2019]

[4] Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II - Center for Strategic and International Studies June 2014. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf [Accessed: 13.02.2019]

The information technology century already requires more consciousness from companies to insure their enterprise risks connected to IT; otherwise, cyber-attacks might cause devastating results such as even bankruptcy.[5] According to the article, (*Ibid*) "as much as 60 percent of hacked small and medium-sized businesses go out of business after six months".

Cyber-insurance product compensates for the financial losses caused by cybercrime and reduces risks to go out of business (more about cyber-insurance see *Chapter 1.1*). Georgia is one step behind to follow world-wide common standards and practices, which is proved by the fact, that a cyber-insurance has appeared in the Georgian insurance market only since 2017.[6] As of today, several insurance companies already provide the product.

Realising, that Georgia is a developing country and, a cyber-insurance only appeared in the Georgian insurance market in 2017 and the "Insurance State Supervision Service of Georgia" has not registered the IT insurance cases in the recently provided statistics, I assume that a cyber-insurance can provide security and stability to the Georgian cyberspace and economy as well as reduce the impact of cybercrime. But, the use of the product should not be low in the country and, every organisation should consider insuring their cyber risks especially the ones who interact with sensitive electronic information massively. Therefore, the master's thesis analyses the influential factors of the product low usage with an objective provide recommendations to improve the use of it.

The study is essential for the region of Caucasian since according to global cybersecurity index Georgia is leading compare to its neighbours (*Figure 1*).[7] Georgia also plans to become a regional provider of cybersecurity services, since the communication systems' infrastructure of the region is located on the territory of Georgia.[8]

---

[5] 60 Percent of Companies Fail in 6 Months Because of This (It's Not What You think), online article. Available at: https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html [Accessed: 07.05.2019]

[6] Available at: https://unison.ge/en/news/cyber-insurance [Accessed: 13.02.2019]

[7] National Cyber Security Index. Available at: https://ncsi.ega.ee/ncsi-index [Accessed: 02.14.2019]

[8] Cybersecurity Strategy of Georgia 2017-2018. Published second time already in 2017. Available at: http://csbd.gov.ge/doc/Cybersecurity%20Strategy_eng.pdf [Accessed: 23.02.2019]

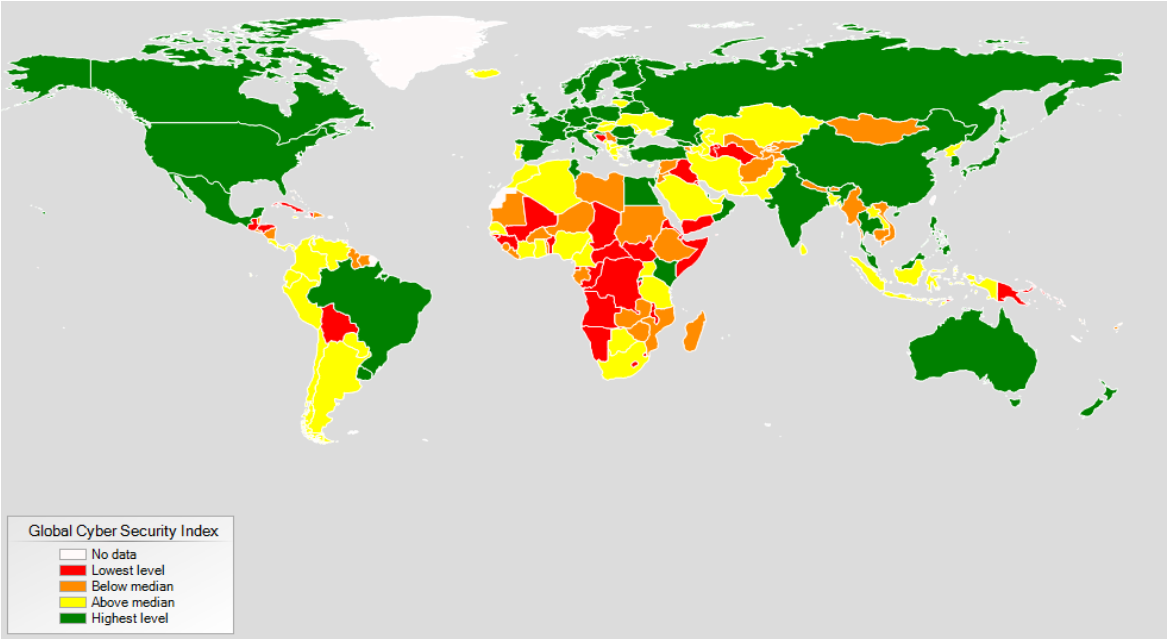


Figure 1. Global Cybersecurity Index. **'International Communication Unit, 2017, "Global Cybersecurity Index (GCI) 2017", July'**

The master's thesis answers to the following questions.

- What are the recommendations to improve the use of cyber-insurance product in Georgia?
  - What is the usage of cyber-insurance in the Georgian insurance market?
    - What are the provided cyber-insurance product characteristics?
    - What are the efforts and ways to increase the awareness and knowledge of cyber-insurance product from insurance companies?
    - Is a cyber-insurance provided for the commercial banks?
  - Do the commercial banks hold a cyber-insurance in Georgia?
    - What are the influential factors of the decision?
  - What issues should be addressed to improve the use of a cyber-insurance in Georgia?

The nature of the master's thesis is analytical; hence the multiple case study has chosen and applied a qualitative approach gathering empirical evidence for analysing and validating the research. The investigation is held via semi-structured interviews.

According to Yin,[9] a case study research is most efficient when the "focus is on a contemporary phenomenon within some real-life context".(*Ibid*) Such an examination is especially relevant in topics which have not drawn much of the researcher's attention (as in our case).[10] There are differentiated two types of case studies; single and multiple. Single is used when dealing with a scarce or critical event and multiple when the information generalisation is needed. (*Ibid*) In this research, the contemporary phenomenon is a cyber-insurance, and some real-life context is the investigation of the product for multiple cases, in the insurance companies and commercial banks.

As for data collection, Eisenhardt describes the following useful methods such are: questionnaires, interviews, observations, and archives.[11] Taking into an account that, the study represents the contribution to the research, I have chosen interviews with predefined semi-structured questions (*see Appendix 1 & 2*) to assemble first-hand experiences, opinions and views from all the respondents. Such open-ended questions give the possibility not to limit the respondent providing with additional information and comment(s). Using semi-structured interviews are considered a preferred option when dealing with the small examples as in this research since they permit a better overview of interviewees.[12]

---

[9] CASE STUDY RESEARCH Design and Methods Third Edition – Robert K. Yin. Available at: https://www.researchgate.net/profile/Ivo_De_Sousa/post/Where_to_get_the_book_Case_Study_Research_Design_and_Methods_by_Robert_K_Yin/attachment/5b4da8f84cde265cb64f9681/AS%3A649298287001611%401531816183878/download/Robert+K.+Yin.+Case+Study+Research-+Design+and+Methods.pdf [Accessed: 13.03.2019]

[10] Recommendations for Using the Case Study Method in International Business Research – Tiia Vissak. The Qualitative Report Volume 15 Number 2 March 2010 370-388. Available at: https://files.eric.ed.gov/fulltext/EJ875260.pdf [Accessed: 13.03.2019]

[11] Building Theories from Case Study Research - KATHLEEN M. EISENHARD. The Academy of Management Review, Vol. 14, pp 532-550. Available at: https://www.uio.no/studier/emner/matnat/ifi/INF5571/v15/timeplan/ar-docs/eisenhardt-1989.pdf [Accessed: 13.03.2019]

[12] QUALITATIVE AND MIXED-METHODS RESEARCH IN ECONOMICS: SURPRISING GROWTH, PROMISING FUTURE - Martha A. Starr. Journal of Economic Surveys (2014) Vol. 28, No. 2, pp. 238–264. Available at: https://doi.org/10.1111/joes.12004 [Accessed: 13.03.2019]

August war in 2008 by the Russian Federation against Georgia, is a grim example of how Georgia was unprepared to extensive cyber-attacks on critical governmental entities, commercial banks, and other informational sources.[13] These cyber-attacks served mainly the idea of cyber warfare, which involved the actions to attack Georgia's information networks and isolate the country in an informational vacuum. Important to outline, that a cyber-insurance has nothing to do with cyber warfare and these facts are provided merely to show, that Georgian commercial banks also were victims of the cyber-attacks during the war. [14] Several Georgian commercial banks were flooded with fraudulent transactions, and as a result, the Georgian banking system went down for ten days. (*Ibid*) This is an excellent example of business disruption and the study researches whether commercial banks in Georgia hold or not a cyber-insurance to get compensation caused by cyber-attacks.

Compared to military operations, which may cause destructive damage, cybercrime is a cryptic and refined threat. Such modern cyber-attacks at first glance are usually unforeseen and underestimated, which require situational awareness and preparedness. Considered that, nowadays dangerous entities for cyber-attacks are commercial banks, stock-markets, atomic electricity generating stations and water compliance systems.[15] Targeted and effective cyber-attack (excluding cyber terrorism and cyber warfare cases) on segments as mentioned above may cause fear, society panic and massive commotion. Cybercrime (for the examples, see *Chapter 1.7*) might produce severe results with a low afford.[16]

According to national security concept of Georgia, reinforcing cyberspace activities to provide and enhance electronic information security, play a significant role in sustainable

---

[13] INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS – Eneken Tikk, Kadri Kaska, Liis Vihul. Available at: https://www.digar.ee/arhiiv/en/download/114641 [Accessed: 13.02.2019]

[14] The 2008 Russian Cyber-Campaign Against Georgia. Available at: https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia [Accessed: 08.05.2019]

[15] SOLVING CYBER RISK PROTECTING YOUR COMPANY AND SOCIETY – ANDREW COBURN, EIREANN LEVERETT, GORDON WOO, pp 12 - 19

[16] კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები - ვლადიმერ სვანაძე, ანდრია გოცირიძე / Main players of cyberspace, politics of cyber-security, strategy and challenges – Vladimer Svanadze, Andria Gotsiridze

economic development.[17] Georgia pays attention to collaborate with its partner countries and share their experience regarding fighting against cybercrime. (*Ibid*)

As stated by cybersecurity strategy of Georgia[18], the primary objective of the country is to create such a system, which will facilitate the protection of informational infrastructure against cyber-threats (to support CIA triad[19]), which on the other hand will be an additional factor for the economic and social development in the country. From seven principles of the strategy, collaboration between state agencies, and, on state and private sectors plays a critical role to defend the ICT[20] sector of the country. A significant part of the vital information infrastructure of Georgia belongs to the private sector, indicating that experience and knowledge existing in this field is mainly accumulated with the private companies. However, worth noting, that addressing the critical information infrastructures under the cyber-insurance coverage represents a complicated and unresolved issue. According to another principle, each citizen, company or public institution should individually ensure security measures internally, under their ownership and management.

Cyber-attacks and technology mistakes potentially can trigger a financial crisis. For instance, flash crashes have been detected on trading exchange platforms as the result of algorithm errors, cryptocurrencies have been hacked and stolen. With help of the "*Kaptoxa*" malware has been stolen more than 40 million debit and credit cards information across the United States, which is the largest scale cybercrime has ever detected in stealing credit card's information.[21] Cyber-attack incidents on banks all over the world indicate that commercial banks remain significantly exposed to cyber threats. Therefore, there are genuine fears, that cyber-attacks can trigger a worldwide financial crisis with a serious negative impact on the global economy. (*Ibid*)

---

[17] საქართველოს ეროვნული უსაფრთხოების კონცეფცია - National security concept of Georgia. Available at: https://mod.gov.ge/uploads/2018/pdf/NSC-GEO.pdf pp. 7, 11, 27 [Accessed: 13.02.2019]

[18] Cybersecurity Strategy of Georgia 2017-2018. Published second time already in 2017. Available at: http://csbd.gov.ge/doc/Cybersecurity%20Strategy_eng.pdf [Accessed: 23.02.2019]

[19] CIA triad – Confidentiality, integrity and availability

[20] ICT – Information and communication technologies

[21] SOLVING CYBER RISK PROTECTING YOUR COMPANY AND SOCIETY – ANDREW COBURN, EIREANN LEVERETT, GORDON WOO, pp 1 – 19, 63- 67

"If cyber-attack succeeds in stealing from large numbers of commercial banks and caused a crisis of confidence by investors in their banks or the values of their financial assets, then the financial crisis could be destructive to society than many other types of the cyber incident". (*Ibid*)

Strong and healthy commercial banking sector helps efficiently direct savings flow and investments in the economy, which eventually accumulates capital by the production of goods and services.[22] According to the online article,[23] "the commercial banking sector is one of the most developed areas of the Georgian economy". Two of the largest commercial banks, TBC Bank[24] and Bank of Georgia[25] are listed on the London Stock Exchange and included in the financial times stock exchange 250. (*Ibid*) That is the reason for choosing the commercial banks in Georgia as a demand-side of a cyber-insurance product since they represent sustainable economic development prerequisite and remain significantly exposed to cyber threats.

The developing countries benefit from the mobile insurance industry, which on its behalf is profitable for the economy. Figure 2 shows, that insurance market activities, banking sector, and economic growth, have the bidirectional connections. The study shows that demands in insurance industry and actions in the banking sector significantly influence per capita economic growth in G-20[26] countries.[27] Georgia is not a G-20's member, but 2019th GDP per capita for Georgia ($4,465) is even higher than for India ($2,305, member of the G-20).[28] Also the world bank's recent statistics about Georgia[29] shows, that

---

[22] Available at: https://www.frbsf.org/education/publications/doctor-econ/2005/january/financial-markets-economic-performance [Accessed: 14.02.2019]

[23] The Rise and Rise of the Georgian Banking sector – Available at: https://emerging-europe.com/georgia-2017/the-rise-and-rise-of-the-georgian-banking-sector [Accessed: 22.04.2019]

[24] TBC Bank – Available at: http://www.tbcbank.ge/web/en/personal-banking [Accessed: 22.04.2019]

[25] Bank of Georgia (BOG) – Available at: https://bankofgeorgia.ge/en/home [Accessed: 22.04.2019]

[26] G-20 Countries – Available at: http://g20.org.tr/about-g20/g20-members [Accessed: 14.02.2019]

[27] Is there a link between economic growth and insurance and banking sector activities in the G-20 countries? - Rudra P. Pradhan, Mak B. Arvin, Mahendhiran Nair, John H. Hall, Atul Gupta. Available at: https://doi.org/10.1016/j.rfe.2017.02.002 [Accessed: 14.02.2019]

[28] GDP by Country 2019. Available at: http://worldpopulationreview.com/countries/countries-by-gdp [Accessed: 14.02.2019]

[29] RECENT ECONOMIC DEVELOPMENTS – GEORGIA. Available at: https://www.worldbank.org/en/country/georgia/overview#3 [Accessed: 14.02.2019]

economic growth of the country accelerates annually. According to "Global Economic Crisis: Is Georgia At Risk?"[30] research, Georgia is not an isolated country, and its economy is sensitive. As a result, the research applies the conceptual framework study for the case of Georgia. The increased demand of a cyber-insurance product[31] and its share into the global insurance industry, conclude an indirect influence of a cyber-insurance product on the country's economic and society welfare.

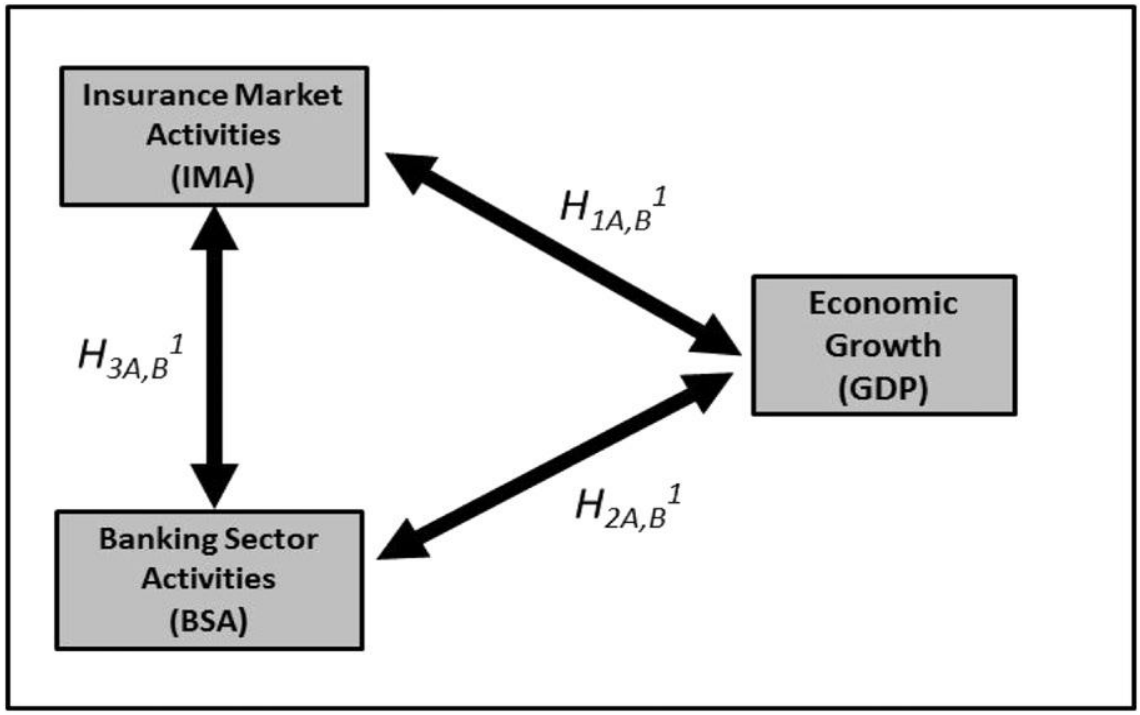


Figure 2. The conceptual framework, how insurance market, banking sector, and economic growth are interrelated. **'Is there a link between economic growth and insurance and banking sector activities in the G-20 countries?'**

Indicator sets have become an essential piece of information, as they provide "a sign or signal that relays a complex message, potentially from numerous sources, in a simplified

[30] Global Economic Crisis: Is Georgia At Risk? – Maka Bughulashvili. Available at: https://journal.ibsu.edu.ge/index.php/ibsusj/article/view/106 [Accessed: 14.02.2019]

[31] Cyber insurance – Statistics & Facts. Available at: https://www.statista.com/topics/2445/cyber-insurance [Accessed: 14.02.2019]

and useful manner."[32] Such resources are essential to guide decision-making, monitoring and evaluation to a study[33] since they contribute valuable knowledge to compound issues in a relatively accessible way.[34] Correspondingly, the conceptual framework illustrates, that indicator sets such are the insurance market activities, banking sector and economic growth (GDP) have the bidirectional connections and influence on each other.[35]

The master's thesis justifies the impact of a cyber-insurance product to economic growth in Georgia as the result of examining the insurance market and commercial banks based on the conceptual framework study. If answers on the semi-structured interview questions indicate that a cyber-insurance impact on reducing costs in commercial banks is significant, the study of conceptual framework will assert that in long-run the product should be influential on per capita economic growth in Georgia.

[32] Evaluation Guidelines for Ecological Indicators. Environmental Protection Agency, Washington, DC 2000. Report No. EPA/620/R-99/005, pp 110 - Jackson, L.E, Kurtz, J.C, Fisher, W.S

[33] OECD, 1993. OECD Core Set of Indicators for Environmental Performance Reviews: A Synthesis Report by the Group on the State of the Environment. Organisation for Economic Co-operation and Development, Paris. Report No. pp 83, 39

[34] A conceptual framework for selecting environmental indicator sets - David Niemeijer, Rudolf S. de Groot. Available at: https://doi.org/10.1016/j.ecolind.2006.11.012 [Accessed: 11.03.2019]

[35] Is there a link between economic growth and insurance and banking sector activities in the G-20 countries? - Rudra P. Pradhan, Mak B. Arvin, Mahendhiran Nair, John H. Hall, Atul Gupta. Available at: https://doi.org/10.1016/j.rfe.2017.02.002 [Accessed: 14.02.2019]

CHAPTER 1: CYBER-INSURANCE PRODUCT

1.1 Basics of cyber-insurance

Cyber-insurance that is known by various names such are cybercrime insurance, IT insurance, IT crime insurance has a broad definition and has been continuously evolving. In 1970 it was defined as the insurance for the physical computer damages,[36] afterwards, starting from 1980 the options of coverage have changed, and cyber-insurance products have designed,[37] but the definition as a risk management tool only appeared in 1990, that has received much of the academic attention over the past decade and a half. (*Ibid*) As of today's formulated concept, cyber-insurance provides compensation to the insured company for the financial losses caused by cybercrime through transferring financial risks associated with network and computer incidents to a third party.

The insurance may be considered as an interesting solution for the cyber threats, as it allows a company to share with insurance provider over many actors the low-probability-high-impact cyber risks, from which each of the actor might be seriously affected by cybercrime, but itself the insured can survive not to go out of business.[38] To strengthen security measures in companies, a cyber-insurance provider might set mandatory requirements on their clients, however there is substantial difficulty,[39] because of high uncertainty of cyber risks, that they are not independent, the way used to be in many other lines of insurance. For instance, the rapid development of IT and business continuity involve many actors who are dependent on each other, hence cyber risks estimation on insurance company's side becomes complicated and challenging. Moreover, cyber-

---

[36] Cyber Insurance - Pythagoras Petratos, Anders Sandberg, and Feng Zhou. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-319-06091-0_25-1.pdf [Accessed: 09.05.2019]

[37] Modeling Cyber-Insurance: Towards A Unifying Framework – Rainer Böhme, Galina Schwartz, 2010 Available at: http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf [Accessed: 28.02.2019]

[38] The cyber insurance market in Sweden - Ulrik Franke. Available at: https://doi.org/10.1016/j.cose.2017.04.010 [Accessed: 10.05.2019]

[39] Models and Measures for Correlation in Cyber-Insurance - Rainer B¨ohme, Gaurav Kataria. Available at: http://sec2013.crysys.hu/~mfelegyhazi/courses/EconSec/readings/09_BohmeK2005insurance_correlation.pdf [Accessed: 10.05.2019]

insurance market existence might be doubtful if the cyber risks are highly correlated (*Ibid*) or insurers are not able to observe customers' security capabilities.[40] As the result of customers' secondary losses such as reputational deface and the high uncertainty of cyber risks, cyber-insurance policies are often overpriced.[41]

On the other hand, a cyber-insurance gives incentives and encourages company to invest in IT security.[42] Under full insurance coverage model self-defense investments are more efficient for cooperative users rather than non-cooperative ones, though partial insurance motivates non-cooperative users to concentrate on investing productively in self-defense mechanisms.[43] According to modelling cyber-insurance unifying framework (*Rainer Bohme, Galina Schwartz, 2010*), cyber-insurance is a robust risk management tool that aligns market incentives toward improving internet security. Over time, cyber-insurance policies have become more comprehensive, since insurers better understand the risk landscape and the business requirements.[44]

The Geneva Association's findings outline, that the cyber-insurance market is still young, but is expected to grow undoubtfully in the upcoming years, and the product is far more advanced in United States rather than in Europe.[45] Many companies in the United States choose to protect their business against cybercrime by buying a cyber-insurance. At least a third of all large organisations in the United States obtain a specific cyber-insurance

---

[40] Competitive Cyber-Insurance and Internet Security - Nikhil Shetty, Galina Schwartz, Mark Felegyhazi, Jean Walrand. pp 229-246, 2010. Available at: http://dx.doi.org/10.1007/978-1-4419-6967-5_12 [Accessed: 10.05.2019]

[41] Why IT managers don't go for cyber-insurance products - Tridib Bandyopadhyay, Vijay S. Mookerjee, and Ram C. Rao. pp 68-73, 2009. Available at: http://dx.doi.org/10.1145/1592761.1592780 [Accessed: 10.05.2019]

[42] Cyber Insurance as an Incentive for Internet Security - Jean BolotMarc Lelarge. pp. 269–290, 2008. Available at: http://dx.doi.org/10.1007/978-0-387-09762-6_13 [Accessed: 10.05.2019]

[43] Analyzing Self-Defense Investments in Internet Security Under Cyber-Insurance Coverage - Ranjan Pal, Leana Golubchik. pp 339-347, 2010. Available at: https://ieeexplore.ieee.org/document/5541674 [Accessed: 10.05.2019]

[44] Managing Organizational Security – Cyber-Insurance in IT Security Management. pp 50-56, 2007. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4218551 [Accessed 10.02.2019]

[45] Ten Key Questions on Cyber Risk and Cyber Risk Insurance – Martin Eling, Wener Schnell, Fabian Sommerrock. 2016. Available at: https://www.genevaassociation.org/media/954708/cyber-risk-10-key-questions.pdf [Accessed: 10.05.2019]

policy.[46] As for the other countries, the interest of cybercrime insurance quickly increases, and cyber-insurance becomes one of the fastest-growing products in the insurance industry. (*Ibid*)

More importantly, the Geneva Association's study claims that, "in general, more empirical research is needed, both on the demand and the supply sides". (*Ibid*) This is another incentive for this master's thesis, to investigate supply-demand side actors in the Georgian cyber-insurance market to develop deeper understanding of reasons with an objective provide recommendations to improve the use of cyber-insurance product.

According to ENISA's report of 2017,[47] coverage types of cyber-insurance can be classified as first party loss, third party loss and other benefits.[48] Figure 3 illustrates the types with the appropriate descriptions. Cyber-insurance policies are mainly spread into two areas: first-party coverage, which covers companies' assets and the third-party cover, which secures the insured from the fallout to affecting the holdings of others as the result of a data breach, fines, etc.

The systems of information technology never are 100% protected. Generally, data on cyber incidents are rare,[49] as there is no standard practice to record them and companies do not have incentives to report either. In the United Kingdom, only 49 cyber-attacks were reported in 2017 to the financial authorities, pointing out material underreporting in the financial sector.[50] In the United States, the SEC[51] published guidance in 2011 on disclosure of cyber risk,[52] which was revised in 2018 to providing additional information

---

[46] SOLVING CYBER RISK PROTECTING YOUR COMPANY AND SOCIETY – ANDREW COBURN, EIREANN LEVERETT, GORDON WOO, pp 235 - 265

[47] ENISA – The European Union Agency for Network and Information Security

[48] Commonality of risk assessment language in cyber insurance - Recommendations on cyber insurance study 2017. Available at: https://doi.org/10.2824/691163 [Accessed: 28.02.2019]

[49] Insurability of Cyber Risk: An Empirical Analysis 2015, The Geneva Papers, Vol. 40 - Biener C, M. Eling and J. Wirfs

[50] Effective global regulation in capital markets, Speech at the ICI Conference, London, 5 December 2017 - Butler, M.

[51] SEC – Securities and Exchange Commission. Available at: https://www.sec.gov/Article/whatwedo.html [Accessed: 28.02.2019]

[52] Securities and Exchange Commission, 2011, "CF Disclosure Guidance: Topic No.2—Cybersecurity"

on how and when companies should reveal the information to investors.[53] Recent successful cyber-attacks such as "Wannacry"[54] in May 2017 and "NotPetya"[55] in June 2017 have shown that cybercrime can lead to severe damage and significant losses for the targeted entities.

Figure 3. Proposed taxonomy of general cyber-insurance coverage components. **'Commonality of risk assessment language in cyber insurance.'**

[53] Securities and Exchange Commission, 2018, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures"

[54] "WannaCry" ransomware attack – Technical intelligence analysis May 2017. Available at: https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf [Accessed: 28.02.2019]

[55] NOTPETYA TECHNICAL ANALYSIS – LogRhythm Labs. Available at: https://gallery.logrhythm.com/threat-intelligence-reports/notpetya-technical-analysis-logrhythm-labs-threat-intelligence-report.pdf [Accessed: 28.02.2019]

1.2 Why to acquire cyber-insurance

For computer science engineers it is tricky to understand the need for cyber-insurance, as they are so used to solve their problems with technologies, but in practice, a business gets security through the insurance industry. Time by time the mindset to secure systems only with technologies slowly changes with the realisation that complete protection does not exist, and the residual risks should be transferred via an insurance product.[56]

Cyber-attacks can impact organisations on the three major information security aspects: confidentiality, integrity, and availability (CIA triad[57]). Confidentiality issues appear when private information is disclosed to a third party as in the case of data breach. Integrity concerns associate with misusing the systems as is the case of fraud, and the availability issues are linked to business disruptions.[58] Business disruptions prevent normal operations of organisation, resulting in lost revenue, while frauds affect directly financial losses, and data breach's one of the significant negative side is that alongside with direct damage it takes more time to monetised since outcomes of reputation costs a lot, but it still presents unsolved issue to compensate losses of prestige in contemporary cyber-insurance market.

Some organisations invest millions of dollars into firewalls, anti-viruses, intrusion detection systems (IDS), etc. to ensure the security of their applications and services. The rapid development of IT produces new viruses and zero-day exploits,[59] which open doors to smart hackers to compromise systems. Cyber-insurance product perfectly fits to cover

[56] Insurance and the computer industry – B. Schneier. Available at: https://doi.org/10.1145/365181.365229 [Accessed: 28.02.2019]

[57] CIA triad – Confidentiality, integrity and availability

[58] Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment – Antoine Bouveret. Available at: https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx [Accessed: 28.02.2019]

[59] Zero-Day exploit – cyber-attack that occurs on the same day a weakness is discovered in software. Available at: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit [Accessed: 02.03.2019]

e-commerce and online organisations delivering e-transactions, since electronic operations are highly exposed to cyber-attacks.[60]

The demand-side of cyber-insurance unite companies which already suffered a data breach and the companies which are just ahead of managing their enterprise risks. There are other categories of organisations, which believe that they are covered by cyber-insurance coverage throughout existing traditional lines of insurance such as commercial general liability (CGL) or property and casualty (P&C), but policy exclusions or policy triggers might ignore the cyber cover.[61] There is also a "silent cover" specifically not excluding cyber threats, but in case of cybercrime, insurance companies might find themselves on the hook of losses not be able to provide a compensation. Successful risk management should estimate cyber risks and decide which residual risks should be outsourced to a third party by buying a cyber-insurance.

1.3 Business perspectives of cyber-insurance

Cyber-insurance unites two main business perspectives: the insurer who is searching to get benefit from premiums exceeding losses over time by spreading the risk of uncertain harmful events across many independent clients and the individual/company who seeks to minimise cybercrime costs by managing the risk of dangerous accidents.[62] Furthermore, calculating premium is a complex process, since the precise estimation of IT-related incidents are not possible because of high uncertainty (*Böhme, Kataria, 2006*). Offering higher rates might give an advantage to concurrent insurance companies while

[60] Cyber-risk decision models: To Insure IT or not? - Arunabha Mukhopadhyay, Samir Chatterjee, Debashis Saha, Ambuj Mahanti, Samir K. Sadhukhan. Available at: https://doi.org/10.1016/j.dss.2013.04.004 [Accessed: 02.03.2019]

[61] Insuring the uninsurable: Is cyber insurance really worth its salt? ISG MSc Information Security thesis series 2017 - Michael Payne, Peter Komisarczuk. Available at: https://intranet.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2017/michaelpayneisg.pdf [Accessed: 02.03.2019]

[62] THE EVOLUTION OF CYBERINSURANCE – Ruperto P. Majuca, William Yurcik, Jay P. Kesan. Available at: https://arxiv.org/ftp/cs/papers/0601/0601020.pdf [Accessed: 28.02.2019]

decreasing the price might keep itself insurance company in danger not be able getting profit by providing coverage.

From the individual's/company's point of view, risk management consists of risk avoidance, mitigation, retention, and transfer strategies.[63] Risk avoidance means not to use information technologies at all, which becomes unprofitable and for most of the organisations already not economically feasible. Risk mitigation is more effective and widely used option to reduce cyber threats by implementing anti-viruses, firewalls and other security measures.[64] Risk retention is mostly the only option for companies with limited financial resources. The companies prefer to take responsibility for the cyber threats they might face rather than transferring the cyber threats to insurance company. As for risk transfer approach, the company accepts, that cybercrime might happen and willing to share the residual risk with a third party by buying a cyber-insurance policy.

1.4 Georgian insurance sector

The economic development in Georgia with ongoing social reforms and consequently, the need for evolution of insurance system in the country has led to adopt the law of "Law of Georgia on Insurance"[65] by the Parliament of Georgia in 2 May 1997. Since then, some amendments and changes have applied to the law, and still, it remains valid.[66] According to latest adjustments (enforced into the law in 20 March 2013[(Ibid)]), the "Insurance State Supervision Service of Georgia"[67] has turned from the subdivision of National Bank of

[63] What do we know about cyber risk and cyber risk insurance? Available at: https://doi.org/10.1108/JRF-09-2016-0122 [Accessed: 28.02.2019]

[64] Critical Security Controls for Effective Cyber Defence. Available at: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf [Accessed: 28.02.2019]

[65] LAW OF GEORGIA ON INSURANCE. Available at: http://insurance.gov.ge/getattachment/Legislation/Normative-Acts/Law_On_Insurance.pdf.aspx [Accessed: 28.03.2019]

[66] Short History of State Insurance Supervision Service Development. Available at: http://insurance.gov.ge/About-Us.aspx?lang=en-US [Accessed: 28.03.2019]

[67] Insurance State Supervision Service of Georgia Available at: http://insurance.gov.ge/getattachment/Useful-Information/List-of-license-documents-eng.pdf.aspx [Accessed: 28.03.2019]

Georgia to legal entity of public law (LEPL) and has become an independent national regulatory entity. The supervision service is independent in its activity and is accountable to the government of Georgia. The "Insurance State Supervision Service of Georgia" has entirely implemented the duties and the responsibilities from the National Bank of Georgia (NBG) in insurance and state pension schema issues.

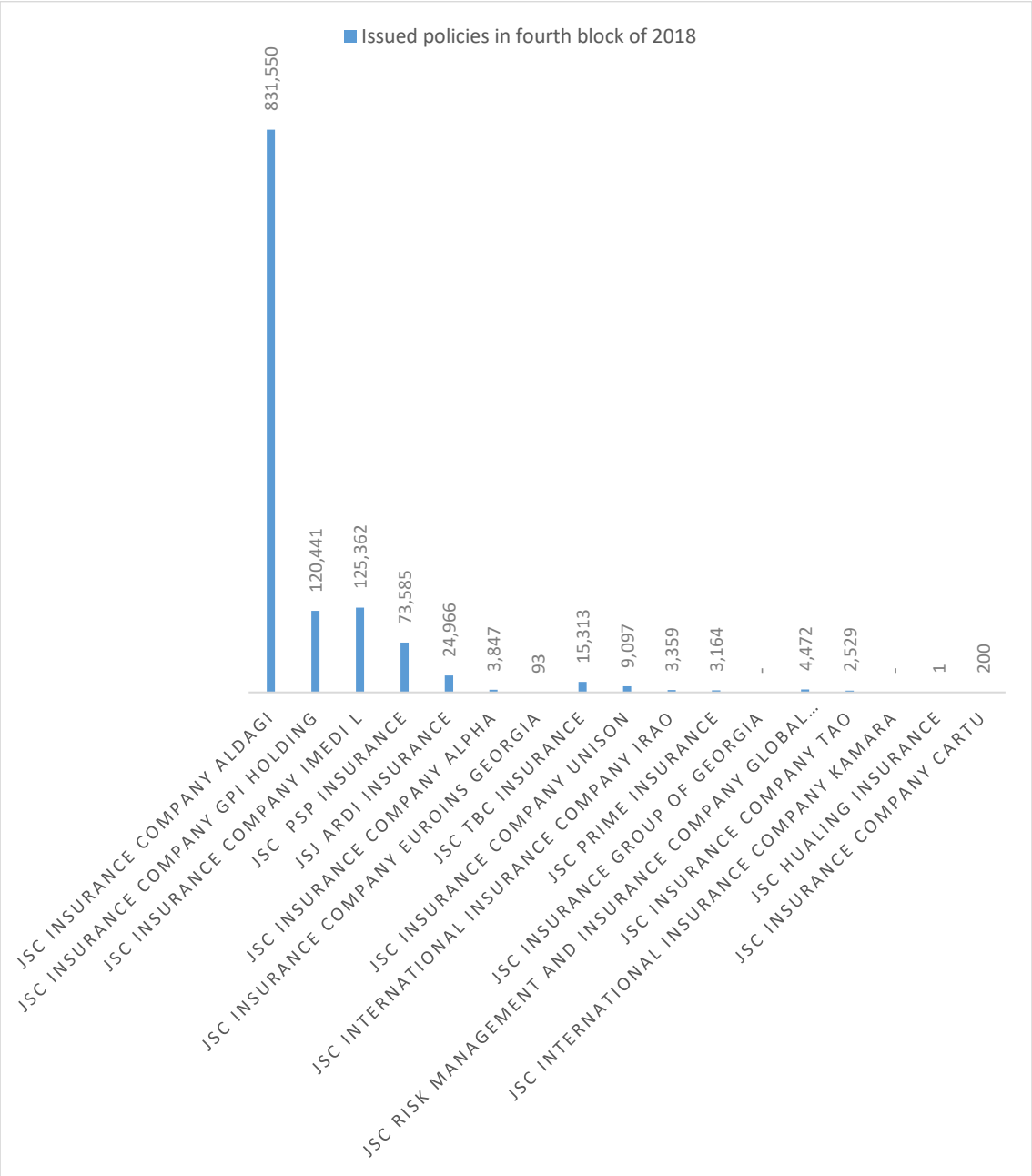


Figure 4. Information on the number of policies (Direct Insurance Business), Reporting Period: 1 January 2018 – 31 December 2018. **'Insurance market statistics. Available at: http://insurance.gov.ge/Statistics.aspx.'**

As reported by "Insurance State Supervision Service of Georgia", there are 17 active insurance companies registered in the country.[68] Figure 4 above shows the latest statistics published by the authority regarding issued policies in the fourth block of 2018.

Figure 5 below illustrates what type of insurance policies are leading on the Georgian insurance market by 31 December 2018. *(Ibid)* It is visible that medical (health), property and road transport are on top of the Georgian insurance market. As for the rest packages the usage percentage is quite low and relatively varying from each other.

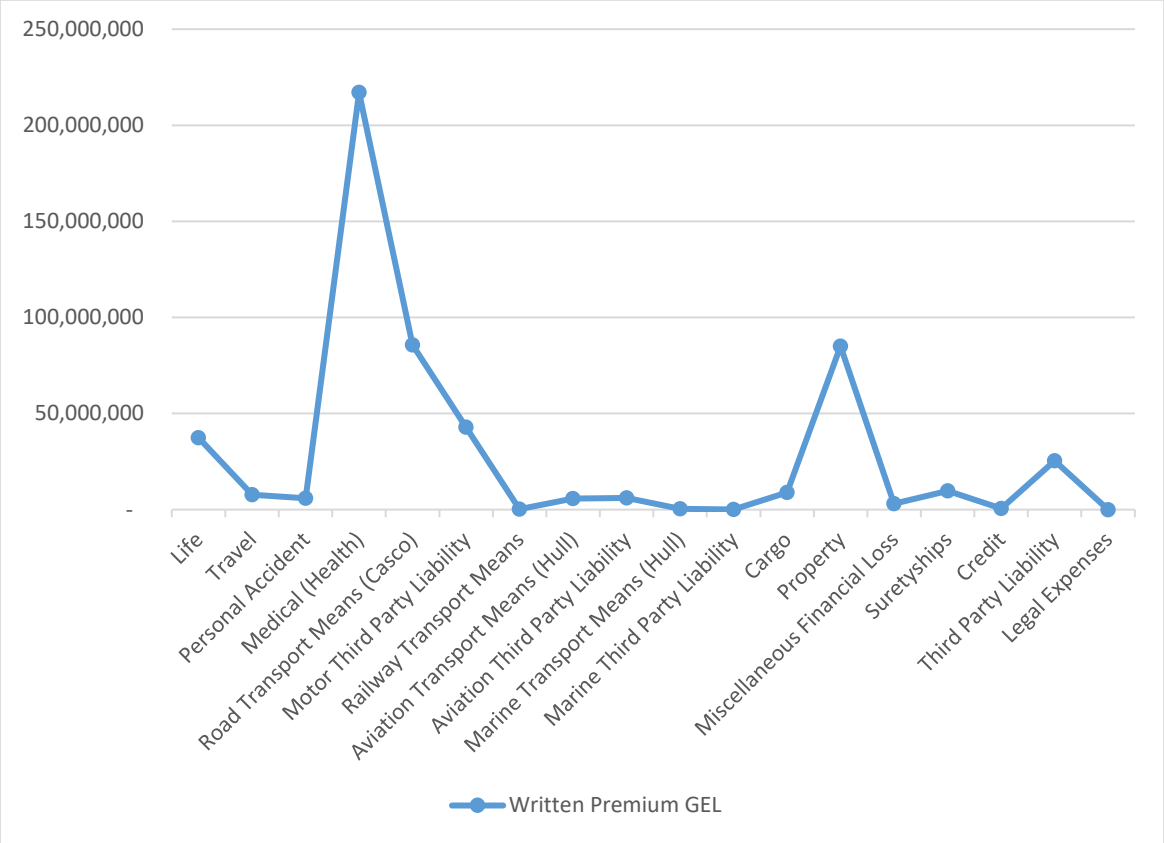


Figure 5. Structure of insurance market by classes of insurance by 31.12.2018 (Direct Insurance Business). **'Insurance market statistics. Available at: http://insurance.gov.ge/Statistics.aspx.'**

[68] Registered insurance companies. Available at: http://insurance.gov.ge/Insurance-companies.aspx?lang=en-US [Accessed: 28.03.2019]

1.5 Evolution of Georgian banking sector

The construction of the Georgian banking sector started in late 1980th when the country was still part of the Soviet Union.[69] After independence declaration in 1991[70] substantive changes have applied to the sector. NBG[71] was established. The commercial banking sector became in chaos in 1994.[72] Assets were emaciated, deposits were lost, society's trustworthiness towards financial institutions was devastated. Banks were often poorly managed and corrupted with no real supervision. (*Ibid*)

Georgia has made very fundamental changes and progress in the commercial banking sector development, to provide the modern banking system and an attractive environment for the investments what is presented nowadays. It remains the fact though that most of the post-communist economies are not very far advanced. The banking sector in Georgia still is in under reforms. Financial institutions should implement modern and standard practices to ensure public trust and economic growth. That is another perspective why study explores the commercial banks in Georgia, to analyse whether they have already implemented a cyber-insurance product or not.

According to NBG in Georgia as of March 2019 there are 15 active commercial banks[73], which are the subject of the study on the demand side of a cyber-insurance. At the very moment, there is no law or regulation which will oblige commercial banks holding cyber-insurance policy.[74] In September 2018 NBG approved corporate governance for commercial banks, which is based on the international practices and standards, including the guide on the management from Basel Committee on banking supervision, principles

---

[69] The Evolution of Commercial Banking in Georgia, 1991-2001 – David Amaghlobeli, John Farrell & James Nielsen. Available at: https://doi.org/10.1080/1463137032000058386 [Accessed: 04.03.2019]

[70] THE CONSTITUTION OF GEORGIA. Available at: http://www.parliament.ge/files/68_1944_951190_CONSTIT_27_12.06.pdf [Accessed: 04.03.2019]

[71] NBG - National Bank of Georgia. Available at: https://www.nbg.gov.ge/index.php?m=130&lng=eng [Accessed: 04.03.2019]

[72] Georgia: from Planning to Hyperinflation - Gurgenidze L, Lobjanidze M & Onoprishvili D, Communist Economies & Economic Transformation 6, 3, 1994, pp. 259–289

[73] https://www.nbg.gov.ge/index.php?m=403&lng=eng [Accessed: 04.03.2019]

[74] ORGANIC LAW OF GEORGIA ON THE NATIONAL BANK OF GEORGIA. Available at: https://www.nbg.gov.ge/uploads/legalacts/fts/eng/on_the_national_bank_of_georgia.pdf [Accessed: 04.03.2019]

of corporate politics of the Organization for Economic Cooperation and Development (OECD)[75], acting directives of the Europe Union (EU) and researchers.[76]

1.6 Banking sector-related cyber risks and incidents

The financial sector remains significantly exposed to cyber risks, including central banks and FinTech companies. In information security risk management, the risk is characterised as a combination of threat levels, exploitation of existing vulnerabilities and consequences.[77]

$$Risk = f(Threat, Vulnerability, Consequences)$$

According to Kopp's study,[78] threat levels are high for financial institutions due to cybercrime, hacktivism, etc. The same goes with vulnerabilities since banks are heavily dependent on highly interconnected networks and critical infrastructures. There are financial institutions, which still are using legacy systems and might not be resilient to modern cyber-attacks.[79] As for consequences, it's easy to realise how destructive might be cybercrime on a bank's reputation, nothing to say about direct losses caused by cyber-attacks. Table 1 shows recent cyber-attacks on central banks all over the world, which on the other hand is a fact to the reason of holding cyber-insurance to get compensation for a cybercrime and not to go out of business.

[75] Organization for Economic Cooperation and Development. Available at: http://www.oecd.org/about/ [Accessed: 04.03.2019]

[76] https://home.kpmg/ge/en/home/insights/2018/09/overview.html [Accessed: 04.03.2019]

[77] International Organization for Standardization, 2011, "ISO/IEC 27005: 011 Information technology -- Security techniques - Information security risk management".

[78] Cyber Risk, Market Failures, and Financial Stability 2017 - Kopp, E., L. Kaffenberger, C. Wilson. Available at: https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx [Accessed: 05.03.2019]

[79] Taking cyber risk management to the next level - Lessons learned from the front lines at financial institutions 2016 - Friedman, S

Institution	Year	Type of attack	Details
Federal Reserve Bank of Cleveland	2010	Data Breach	Theft of 122,000 credit cards
Federal Reserve Bank of New York	2012	Data Breach	Theft of proprietary software code worth USD 9.5 Million
Sveriges Riksbank	2012	Business disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
Banco Central del Ecuador	2013	Fraud	USD 13.3 Million stolen from the account of the city of Riobamba at the central bank
Federal Reserve Bank of Saint Louis	2013	Data Breach	Publication of credentials of 4,000 US bank executives by Anonymous
Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000
ECB	2014	Data Breach	20,000 email addresses and contact information compromised
Norges Bank	2014	Business disruption	The DDoS attack on seven large financial institutions, resulting in suspended services during a day
Central Bank of Azerbaijan	2015	Data Breach	Theft of thousands of bank customers information
Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer USD 81 Million from its account

			at the FRBNY. Hackers tried to steal USD 951 Million
Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million
Bank of Italy	2017	Data Breach	Hack of email accounts of two former executives

Table 1. Recent cyber-attacks on central banks. **'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment – Antoine Bouveret'**

According to online article,[80] financial losses caused by frauds in the banking sector rose to 2.2 billions of dollars in 2016, which is 16% increase from 2014. Such fraudulent operations represent quite a big concern for the banking industry. Tendency of fraudulence rises and never stops. Moreover, it is not only about banks, but general. For example, IC3's report claims, that in 2018, 14,408 complaints were victims of tech support fraud in 48 countries, resulting in nearly 39 million of dollars losses, which represents 161% increase from 2017.[81]

Taking into consideration that the IT evolves rapidly, and no entity ever be entirely sure in their possibilities to secure the information systems, and the facts as mentioned above are reality regarding cyber-attacks on central banks all over the world, it is always a good option transferring financial risks related to computer and network incidents to a third party by taking out a cyber-insurance.

[80] Frauds in banking industry. Available at: https://financialregnews.com/banking-industry-suffered-2-2-billion-fraud-losses-2016 [Accessed: 10.05.2019]

[81] 2018 INTERNET CRIME REPORT. Available at: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf [Accessed: 10.05.2019]

CHAPTER 2: THE REASONS FOR THE LOW USE OF A CYBER-INSURANCE PRODUCT IN GEORGIA

2.1 Overview

The following subchapters outline the data collection details and analyse the received feedback. Based on gathered empirical evidence has taken from the interviewees, the cross-case tables are used to proceed cross-case analysis; namely to differentiate similarities and differences in the received answers, to summarise cyber-insurance usage in Georgia, its characteristics, awareness and knowledge, and the reasons that should be addressed as the recommendations to improve the use of cyber-insurance.

2.2 Data collection

I have moved to Georgia to gather first-hand experiences, views and opinions from the insurance companies and commercial banks. The reasoning of moving is explained merely by the fact, that collecting the data from the informants are more comfortable, take less time and most importantly is reliable to have a face-to-face interview. Below subchapters describe communication details, how many informants have contacted, by what means, etc.

2.2.1 The informants of insurance companies

In the Georgian insurance market as of March 2019, there are 17 active insurance companies.[82] Firstly, internet resources were used to collect general information about the insurance companies. For instance, on what kind of insurance product is a company specialised and what type of insurance packages are provided. The quick research[83] (was

[82] Licensed insurance company register in Georgia. Available at: http://insurance.gov.ge/Insurance-companies.aspx [Accessed: 30.03.2019]

[83] I visited each insurance company's official web page and checked their experience on what kind of insurance segments they are specialised.

done through the web) was rechecked by direct calling to the company's call centre to clarify the assumptions. Turns out, that "PSP insurance"[84] and "Imedi L"[85] insurance companies are specialised only in the healthcare industry. Therefore they were eliminated from the research. Other 15 organisations were added on the spreadsheet of the applicable actors for the study. Started from March 18, 2019, all the relevant candidates have been contacted with the proper email in English (attached the student certificate from the TUT[86]) (see *Appendix 3*), indicating the purpose and reason of the letter. Only 2 of the actors responded within the week on the email, for other 13 companies I had to call or directly visit the main branch offices for the feedback. In total, I received answers from 8 insurance companies, including 2 of them providing a cyber-insurance product. As for other seven entities, they have not answer on the email and during calling to their call centre, I was told that they do not provide the product and thus they do not have anything to say regarding the interview questions.

2.2.2 The informants of commercial banks

To get feedback from the commercial banks Compared to insurance companies turned out less successful due to the nature of the interview questions. Contact email has written in English was sent to all the major banks in Georgia,[87] (attached student certificate from the TUT) (see *Appendix 4*) was described the purpose and reason of the study with the note, that interviewee is not limited providing any relevant information or even skip the inquiry in case of need. I have managed to get answers only from two banks. One another bank responded that the letter had been sent to the relevant service and in case of interest they would be in touch within two weeks interval. They have not sent any feedback though. Likewise, none of the remaining banks showed their enthusiasm contributing to

[84] "PSP Insurance". Available at: http://ipsp.ge [Accessed: 30.03.2019]

[85] "IMEDI L". Available at: https://www.imedil.ge/en/about-company [Accessed: 30.03.2019]

[86] TUT – Tallinn University of Technology

[87] List of Active Commercial Banks. Available at: https://www.nbg.gov.ge/index.php?m=403&lng=eng [Accessed: 30.03.2019]

the research. Calling to call centre of the banks were ended with the same answer to wait for feedback on the email.

The inactivity of the banks for the contribution to the study on relatively sensitive IT security information can be explained with the unrevealed cybercrime facts on TBC.[88] According to the article[89] and to publicly disclosed information, cyberattack on the bank happened in 16 July 2018, which was notified next day to the ministry of internal affairs[90]. Nonetheless of the outstretched investigation, according to recent article[91] inspection has not been interrupted and complex examinations are still ongoing. As reported by a deputy of minister of internal affairs, the information will become openly available as soon as there are concrete results. *(Ibid)* In such case, there is no wonder that, none of the banks willing to share their IT[92] security information especially then when there is still unsolved cybercrime issue.

2.2.3 Interview situation

The head branch offices of all the actors are located in the capital of Georgia, Tbilisi.[93] Only one face-to-face interview was managed to proceed in English; others were conducted in Georgian.

On insurance company's side, five interviews were held face-to-face. As for the remaining 3 actors, communication was done on the phone, but worth noting that none of these was a cyber-insurance product provider. Hence they have not had much to say anyway.

---

[88] One of the largest commercial Bank in Georgia. Available at: http://www.tbcbank.ge/web/en [Accessed: 30.03.2019]

[89] Cyberattack on TBC on July 16, 2018. Available at: https://www.bm.ge/ka/article/tbc-ze-kibersheteva-2018-wlis-16-ivliss-ganxorcielda---tbc-is-werilebi-gasajarovda/31094 [Accessed: 30.03.2019]

[90] Ministry of Internal Affairs. Available at: https://police.ge/en/home [Accessed: 30.03.2019]

[91] Deputy of Minister of Internal Affairs comment on cybercrime on TBC. Published on March 18, 2019. Available at: https://news.ge/kibersheteva-tbcze [Accessed: 30.03.2019]

[92] IT – Information technology

[93] Georgia situates in the south Caucasian region in the greater Caucasian mountain range.

As for the commercial bank's side, one interview was managed as face-to-face, and another one was proceeded only via email. It worth noting, that before getting the feedback from the last bank mentioned above, I was called by the bank's representative to clarify details regarding the purpose of the research. The bank's representative was explained about privacy issues, that the bank's name wouldn't be disclosed during writing the master's thesis since the study aims to get only general information about a cyber-insurance and the use of the product in the commercial banking sector.

The interviewees had received interview questionnaires via email beforehand the meeting. They were offered to see the questions from the laptop during the communication process and were asked consent regarding recording the audio, explained the need of it, but I was allowed to do so only with one actor on insurance company's side, for which interview was held in English. As for the other cases, where the recording was disallowed, I had to write down notes during the conversation.

I followed predefined guidelines during the interview process, but time to time questions order were changed, and minor modifications to the questions were happened. That is another aspect of semi-structured interview practice to concentrate and elaborate on the related topic of the conversation. At the end of the meeting, I thanked the interviewees for their time, and the feedback, and invoked them feeling free providing subject related views, opinions or comments.

2.3 Data transcription

The digital audio-recording was done with the help of "Otter.ai"[94]. The application is available on a mobile device and web interface, which facilitates transcription of audio-recording automatically with the help of artificial intelligence. As of March 2019, transcription was only supported for the conversations were held in English. According to the official web page, "Otter.ai creates technologies and products that make information from important voice conversations instantly accessible and actionable." (*Ibid*) The application is quite easy to use and effective for the research, not to lose time on

[94] AI for everyday conversations. Available at: https://otter.ai/about [Accessed: 31.03.2019]

writing down notes and not to miss conversation details. The user can highlight, edit, copy, and export text, as well as generating a word cloud. Audio importing, repeating, speeding up and down gives the possibility to concentrate on the conversation details and make it useful for the analysis.

In an ideal situation, all the conversations should have recorded in English with the application mentioned above, but according to informants' consents, only one interview has been recorded so. Figure 6 shows the taped transcription of the conversation from the web interface.

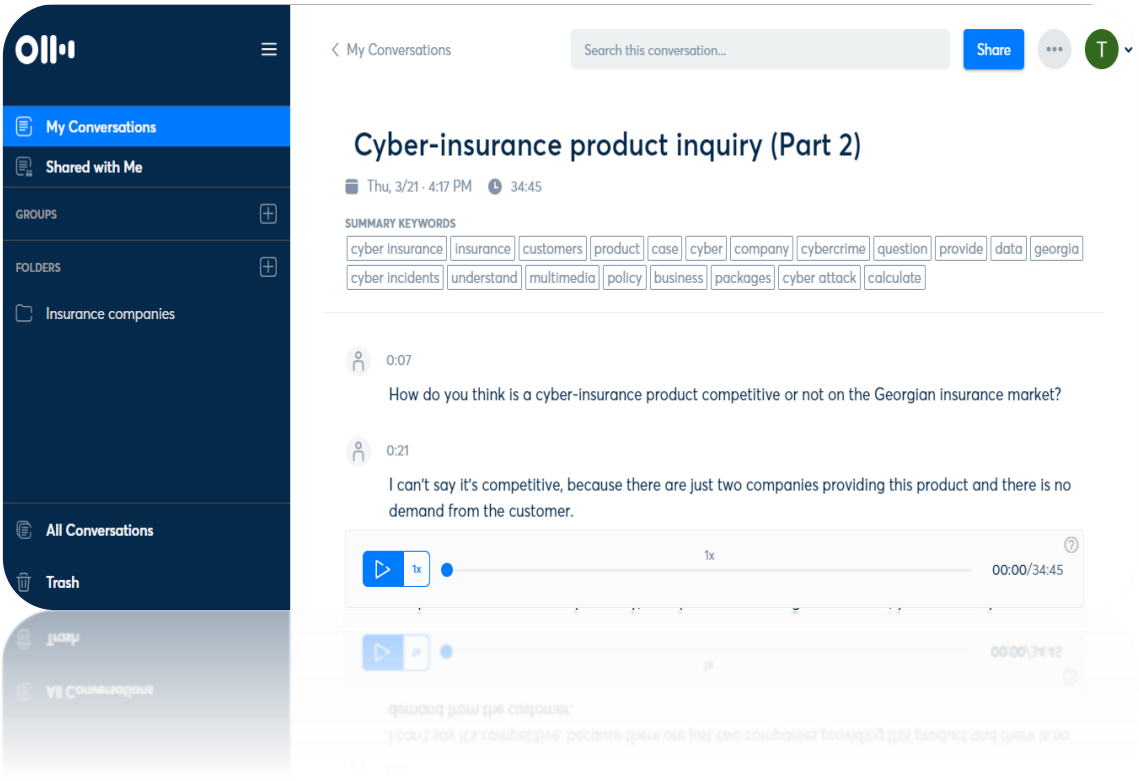


Figure 6. Cyber-insurance product inquiry audio transcription from the insurance company.

As for the interviews for which audio recording was disallowed, the traditional approach of writing down the quick notes directly into the word document was used. As soon as the interview process was done and farewelled the informants, I made up my mindset to remember all the details from the conversation and wrote eloquent notes into the document, not to forget significant points of the speech.

2.4 Ethics

The introduction email was sent to each of the applicable entity, presenting myself and the research topic with the attached student certificate from the Tallinn University of Technology alongside with interview questionnaires. During the face-to-face interview process, I have presented an ISIC[95] card with the printed-out student document from TUT[96] once again to give interviewee possibility to verify myself easily and be confident on my identity and the research purpose. I was open answering additional questions from the informants regarding the subject of their interest.

For the phone conversations to the informants, I still have explained my status from the university and the purpose of study. All these communications were done with insurance company's representatives whose organisations do not provide a cyber-insurance product, hence on answering none sensitive questions were not much of the deal going into the details on my identity from the informants.

2.4.1 Anonymisation

Due to relatively sensitive interview questions to the bank's representatives regarding cyber-insurance product and the information technology security issues, all the data collected from the commercial banking sector are being anonymised, meaning that no names of the informants or their banks are being revealed. Such privacy plays a critical role in the bank's security regulations. Georgia has a small market and giving out much of the information might provide the possibility to a misuser to have an educated guess identifying the informant or the company itself.

As for the insurance companies, I have decided to anonymise the names of the informants and the organisations which do not provide a cyber-insurance product, since the answers from their interviewees might give some advantage to their competitor companies. For the insurance companies offering a cyber-insurance product by their representative's

[95] ISIC - International Student Identity Card. Available at: https://www.isic.org/about-us [Accessed: 31.03.2019]

[96] TUT – Tallinn University of Technology

consents, the names of the organisations are being revealed. The information regarding providing a cyber-insurance product are publicly available and even represents a marketing public relations (PR). It is doubtful that the confidential information is being disclosed, even if some of the data given by informants are not publicly accessible. Revealed company's representatives were given the possibility to correct the interpreted information I have described from the interview transcripts into the results of the master's thesis.

2.4.2 Recorded audio handling

I was given the consent by the informant of recording the audio on "otter.ai"[97] only from one insurance company. It was explained and decided that the audio only be used by me while writing the research paper, would not be disclosed to anyone and would be deleted as soon as the work is done. According to the application's privacy policy,[98] no record will be retained by "AISence"[99] as soon as the data are removed by the user who uploaded the audio, in this case by me.

2.5 The naming conventions for the companies

I have decided to give the alias names for the insurance companies (except the ones who already provide a cyber-insurance) not to reveal their attitude and plans to their competitors. Names such are A1, A2, etc., has chosen for the risk taker of the last resort organisations. As for the commercial banks, due to sharing a relatively sensitive IT security information their names are represented by B1 and B2.

For the feedback received from the informants with views, opinions and examinations, please check the following subchapters.

---

[97] AI for everyday conversations. Available at: https://otter.ai/about [Accessed: 31.03.2019]

[98] Privacy Policy of "Otter.ai". Available at: https://otter.ai/privacy [Accessed: 31.03.2019]

[99] AISense Inc. is the company name of the otter.ai application.

2.6 The feedback of insurance companies

Nowadays on the Georgian insurance market only "ALDAGI"[100] and "UNISON"[101] provide a cyber-insurance product. As for other companies except one do not exclude the possibility of offering cyber risk insurance for the future, though they don't have any specific plans as of April 2019. Table 2 illustrates a brief overview of the inquired informants.

Insurance company	Academic background and position	Experience in the insurance industry and company	Reinsured	Cyber-insurance product	Planning to provide a cyber-insurance shortly
ALDAGI	Bachelor of Business Administration. Head of Marketing && PR Division	15 years && 12 years accordingly	YES	YES	Already providing
UNISON	Bachelor of Business Administration. Head of Marketing Department && Leading Cyber-Insurance Product Team	2 Years in both	YES	YES	Already providing
A1	Management, Head of sales management	2 Years in both	YES	NO	NO
A2	Marketing, Marketing manager	3 Years in both	YES	NO	NO
A3	Marketing manager	1 Year in both	YES	NO	NO
A4	Marketing manager	1 Year && 2 Months accordingly	YES	NO	NO
A5	Brand manager	1 Year in both	YES	NO	NO
A6	Marketing manager	1 Year in both	YES	NO	NO

Table 2. Cross-case table - Insurance companies overview.

[100] "ALDAGI". Available at: http://aldagi.ge/en [Accessed: 02.04.2019]

[101] "UNISON". Available at: https://unison.ge/en/about-us [Accessed: 02.04.2019]

ALDAGI. According to the publicly available online article,[102] head of corporate sales department David Ejibia stated, that recently in Georgia have detected many cybercrime cases and a lot of companies have suffered from it. These results have given motivation to "ALDAGI" to create a cyber-insurance product that can help organisations to get compensation for the cybercrime losses. He emphasised that the insurance company can handle massive damage caused by cyber-attacks. (*Ibid*) The interviewee told the same that "ALDAGI" concentrates on giving out the cyber-insurance policies on the big organisations including commercial banks, but they do not limit any size of entities or even individuals from taking out cybercrime coverage.

The interviewee indicated that "ALDAGI" created a cyber-insurance in 2017, mainly for the image purposes and provides the product only in the Georgian insurance market. Based on the general market analyse, which takes place every five years, the respondent told that as of April 2019 the product in the Georgian market is not competitive or demandable. The company's other article[103] outlines the same that by the time of publishing the information they only had had one policy and ongoing negotiations with another customer. The informant considered that the product is new in the Georgian insurance market with a low awareness and knowledge on the demand side. The respondent told that public relations of the product only have happened with their already existing customers (who hold other type of insurance packages) and "ALDAGI" has not tried yet to promote a cyber-insurance massively in public.

The interviewee emphasised that a cyber-insurance is a high-risk profile insurance product, that is more challenging to estimate and set premiums compared to other products. With the same reason, that cybercrime insurance is new for the insurance market in Georgia and there is almost no demand from the customer's side, the company does not have claims experience for the product. The informant believed that in case of cyber incidents against their customers, the clients will notify "ALDAGI" regarding it since the

---

[102] How to protect from cyber-attacks to minimize loses to a minimum, online article, published on: 23.02.2018. Available at: https://on.ge/story/17193-%E1%83%90%E1%83%9A%E1%83%93%E1%83%90%E1%83%92%E1%83%98 [Accessed: 03.04.2019]

[103] Cyber-Insurance – "ALDAGI"'s unique offer to a customer, published on: 28.09.2017. Available at: https://www.interpressnews.ge/ka/article/454804-kiberdazgveva-aldagis-unikaluri-shetavazeba-momxmarebels [Accessed: 03.04.2019]

company's agreement requires such information sharing. The respondent did not exclude the possibility of information sharing with appropriate government entities and their reinsurers. According to the interviewee, demanded claims are always checked against fraud. "ALDAGI" investigates a candidate customer and based on risk assessment grants or rejects the cyber coverage. Worth to notice, that the interviewee assumed that for the long-term a cyber-insurance will become demandable product in Georgia and it will have an influence on reducing financial losses caused by cybercrime. The respondent's argument for such assumption is the increased cybercrime cases in Georgia and growing tendency of cyber-attacks.

UNISON. The interviewee explained that the company started to offer a cyber-insurance in the Georgian insurance market in 2017. The company looking forward to concurrent cyber-insurance market, as it promotes the product.[104] "UNISON" is fully backed up by world's A+ ranking reinsurer companies, that gives more confidence and reliability to deal with many low-probability-high-risk profile subjects. (*Ibid*) According to the respondent, cyber-insurance packages are 100% reinsured by AIG[105] insurance organisation. The informant told that the product is not competitive in Georgia, and a cyber-insurance mainly was created for reputation purposes. Nonetheless, that the demand is not high, the company's representative believed, that offering a quality product with proper explanation will eventually increase the awareness and the need. (*Ibid*)

The informant outlined about one of the significant factors of a low demand, which is none existing regulations for the data protection, like, "General Data Protection Regulation",[106] which enforces organisations protect and proceed their customer's data more strictly and transparently by the permitted consent. It was told that the company is more interested and concentrated to cover big organisations including financial institutions, commercial banking sector, etc.

---

[104] Online article. Available at: https://unison.ge/en/news/cyber-insurance [Accessed: 04.03.2019]

[105] AIG – Official web page. Available at: https://www.aig.com/about-us [Accessed: 04.03.2019]

[106] GDPR – General Data Protection Regulation. Available at: https://gdpr-info.eu [Accessed: 03.04.2019]

"UNISON" may set security regulations and requirements to a customer. A premium is low in case security measures are satisfied. As for the public relations of a cyber-insurance, the company tries to promote the product by direct sales and email marketing, but the public promotion has not done yet.

The interviewee stated that they do not have any claims yet for a cyber-insurance since it is entirely new and not many companies are interested in. The quantity of a cyber-insurance policy holders was not specified, though it was told that the number is very low. Regarding, information sharing, the respondent told that they have obligations towards appropriate government structures to share cyber incidents with them. The informant considered that nowadays a cyber-insurance does not have any impact on reducing cybercrime costs in Georgia, as the product is only just starting to implement into the Georgian insurance market, but in couple of years after, a cyber-insurance should have influence already on diminishing the financial losses.

A1. According to the interviewee, the company systematically (quarterly) analyses the Georgian insurance market, though, with the simple reason that there is no demand, the company does not provide a cyber-insurance product. The informant explained also, that they do not concentrate on high-risk profile insurance packages and have not tried anything to increase awareness of the product. As stated by the respondent, they are not going to implement a cyber-insurance package shortly, but if insurance market requires, the company will consider to offering the product for the long-term perspectives.

A2. As reported by the informant, a cyber-insurance product is not spread in the Georgian market so that it is worth to offer. The Company analyses the Georgian market systematically (quarterly, annually and based on manual indications of the management) and follows a common tendency providing saleability products, but there are no such demands from the customers, which would give incentive to the organisation to offer a cyber-insurance product. The manager did not exclude the possibility of implementing the cyber risk insurance for the future, as soon as the company considers that demands are such high to get benefits from providing it.

A3. I had communication with the company's marketing manager on the phone and surprisingly got unexpected feedback, that the informant could not find a competent person who would be able to answer the interview questions. The manager mentioned

that they not only do not provide a cyber-insurance, but they don't know what it is at all. The manager asked me if anyone in Georgia provides such product.

A4. The marketing manager of the insurance company explained that they don't provide a cyber-insurance product with the same reason, that there is no customer's demand in the Georgian market. The manager remembered, that the company was providing a cyber-insurance for some time ago, though they stopped offering high-risk profile packages because of not profitable demands from the customer's side. The manager emphasised that the company willing to provide the product, but only then when demands will worth to satisfy.

A5. According to the brand manager of the insurance company was stated that the company systematically analyses the Georgian insurance market, monthly for existing customers and annually for the whole market. The company does not offer a cyber-insurance product, as there is no demand in the market. The company tries to be an innovator but does not provide IT insurance and furthermore, has not done anything to increase cybercrime insurance knowledge and awareness among IT companies nor with individuals. The brand manager mentioned that they will be happy to offer a cyber-insurance in long-run when there is a need for it.

A6. Marketing manager of the company explained that with current demands in the Georgian insurance market there is no need of providing a cyber-insurance product. The company does not concentrate on insuring high-risk profile subjects, and it does not worth for the organisation to implement product even only for the reputation. If in future a cyber product becomes demandable, they will consider to offering a cyber-insurance.

2.7 The feedback of commercial banks

I have managed to get feedback only from two commercial banks from in Georgia. One interview was held by face-to-face communication, as for the other, answers were received on the email. However, worth to mention that none of the feedback answers all the questions entirely, once again due to relatively sensitive cybersecurity information.

Question/Bank	B1	B2
Position in the bank	Head of the cybersecurity department	Head of the information security department
The bank should have acquired a cyber-insurance	Yes	Yes
Risk management strategy	Risk mitigation	Risk mitigation Partially Risk transfer
Cybersecurity department	Yes	Yes
The bank holds a cyber-insurance policy	No	Fraud
Risk management is aware of cyber-insurance	Yes	Yes
Cyber-insurance helps to increase customers' trustworthiness towards the bank	No	No
The bank plans to acquire a cyber-insurance	Yes	Yes
Reasons of buying a cyber-insurance policy	Safety, reliability, regulations, increased cybercrime tendency	Safety, reliability, world-wide common practices, regulations, increased cybercrime tendency
Type of cyber incidents that willing to be covered	Business Disruption Data Breach Fraud	Business Disruption Data Breach
The bank has been the victim of cyber-attack(s)	Not specified	Not specified
Experience of such cybercrime case(s) when cyber-insurance would be useful	No	No
Will a cyber-insurance make an influence on cybersecurity department operations	No	No
The attitude of cyber-incidents' information sharing	Negative	Negative

Table 3. Cross-case table - Bank's profiles.

B1. The head of the cybersecurity department officer agreed that nowadays in the real-world a business should be protected throughout the insurance industry, especially financial institutions. The bank does not hold any insurance (excluding the property insurance), and the interviewee explained that the bank at the very moment only uses risk

mitigation strategies, protecting their information systems with technology means such are firewalls, IDS[107], following common frameworks, etc. The risk management is aware of a cyber-insurance product, the packages which are available on the market and they are working to acquire them. As for the problematic aspects of buying a cyber-insurance, the respondent was not clear on reasons, but it was told that risk management was slow to promote the issue on the timetable. The Georgian practice and tendency of cybercrime cases can justify the reason, that the cyber-attacks have not happened before so often like nowadays. The informant noticed that risk management and cybersecurity department are not enough to resolve the issue and it should be agreed on the upper management layers. The interviewee showed a positive attitude to provide recommendation to the top management to set a cyber-insurance as a must have directive for the bank. According to the respondent, the bank is in need of holding cyber-insurance policies against business disruption, fraud and data breach. The informant told that owning the coverage would not make any influence on cybersecurity and risk management operations, and they will remain sufficient. Worth noting, that according to the respondent, they prefer to take out a cyber-insurance from foreign insurance company rather than from the local one, even though insurance companies in Georgia are already fully backed up by world's leading reinsurer organisations and ready for challenges. This fact was merely explained that the trustworthiness and experience are higher for the foreign companies than for the local ones. The bank follows world-wide common technology standards and frameworks, though I did not get an answer on whether the bank conducts or not a penetration testing, neither has ever the bank experienced the cyber-attacks. Though, it was told, that up for now, the bank had not had such case where a cyber-insurance would be useful. As for the information sharing, the respondent expressed his opinion that the bank won't share information of cyber incidents unless regulations oblige them. On the other hand, they are always welcome to get the information from others and share their experience. The informant confirmed that the bank is on its way of taking out cyber-insurance, but the time of the acquisition phase might take was not specified.

B2. The head of the information security officer gave feedback to me on the email and mentioned that the bank only has insurance against the frauds. That, risk management is

[107] IDS – Intrusion detection system

aware of the other type of cyber-insurance packages and they are on the way of implementing them. The officer indicated that up to his knowledge the National Bank of Georgia works on new regulations regarding cybersecurity towards the commercial banking sector, however the regulations are not in force and also are not publicly available. According to the officer, the bank uses mainly risk mitigation strategy, technology means (antiviruses, firewalls, IDS, etc.) to reduce the chance of the cyber-attacks. As for the fraud insurance package, it covers financial losses caused by frauds and the bank is partially using risk transfer strategy as well. B2's representative believed in the necessity of business disruption and data breach insurance packages. According to him they won't increase the trustworthiness of the customers and won't make any influence on internal information security operations though. The informant explained that the bank had not experienced any such case where a cyber-insurance would be handy. If cyber-attacks have ever happened against the bank were not specified, neither was told whether the bank periodically does penetration testing or not. As for the information sharing, their bank won't disclose cybercrime events unless they are obliged to do so. But getting information from other organisations in mitigating and avoiding the cyber-attacks are always welcome. Worth to mention, that according to the respondent, the bank nowadays assessing the risks, therefore not all of them are defined and estimated. Firstly, it is critical for the bank to finish risk assessment and then identify the ways how to handle them. In the end, the informant confirmed, that nowadays Georgian reality already demands a cyber-insurance and they will eventually take it out since only risk mitigation strategy is not enough. How much time a cyber-insurance acquisition phase might take remained unanswered though.

2.8 Results

2.8.1 The characteristics of cyber-insurance

All the investigated insurance companies, except the ones that provide a cyber-insurance are eliminated from the cross-case table 4, which illustrates similarities and differences of a cyber-insurance between "ALDAGI" and "UNISON".

Question/Insurance company	ALDAGI	UNISON
Company established in	1990	2011
Cyber-insurance	Yes	Yes
Cyber-insurance product is fully reinsured	Yes	Yes
Offers the cyber-insurance since	2017	2017
The main reason for providing a cyber-insurance	Reputation	Reputation
Estimated cyber-insurance awareness and demand on the Georgian market	Low	Low
Concentrated offering a cyber-insurance to	Mainly big companies rather than individuals	Mainly big companies rather than individuals
Providing a cyber-insurance for the commercial banks in Georgia	Yes	Yes
Coverage	Network Interruption Network Interruption OSP System Failure Cyber Extortion Electronic Data Incident Data Restoration Extra Expense System Clean-up Costs Administrative Investigation and Penalties Data Protection and Cyber Liability Wrongful Collection of Information First Response	Network Interruption Network interruption OSP System Failure Cyber Extortion Electronic Data Incident Data Restoration Extra Expense System Clean-up Costs Administrative Investigation and Penalties Data Protection and Cyber Liability Media Liability Wrongful Collection of Information First Response

		Communication Costs
Public Relations (PR)	Only with customers' companies	Only with customers' companies
The quantity of sold cyber-insurance policies	1 based on online article, however the number was not specified by the respondent	Not specified
Claims	No	No

Table 4. Cross-case table – A cyber-insurance product similarities and differences provided by insurance companies in Georgia.

The table 4 is created based on the interviewees' feedback and their presentations. The cross-case table shows that the insurance companies offer almost the same cyber-insurance coverages, with the difference, that "UNISON" also provides media liability and communication costs compared to "ALDAGI". "ALDAGI" has an individual approach to customers and the coverage packages can be negotiated with clients. Same is true for "UNISON"', that they try to concentrate on the client's needs, but that they do not cover "Cyber Theft" (for example, if money is transferred from hacked accounts to elsewhere) since it's quite tricky to investigate.

The received feedback confirms that a cyber-insurance product covers first-party and third-party losses, and provides other benefits, for instance: first response (Crisis management, IT experts, Breach-related legal advice, etc.), communication costs (following damage to reputation). Nonetheless, that as of today there is no much of demand and experience of a cyber-insurance in the Georgia, insurance companies are willing to provide the product to commercial banks and other organisations who are dealing with the information systems massively. Considering the facts, that cyber-insurance is 100% reinsured by world's leading insurance companies, it strengthens reliability and confidence of the product in the Georgian insurance market.

The cross-case table analysis points out that a cyber-insurance product is mainly implemented for reputational purposes. The product has been offered since 2017, and in

the companies' online articles[108], both of companies are claiming that they were first providers of cybercrime insurance. The product is not much tradable, but a cyber-insurance market is already designed, which on its behalf is the guarantee for the product development. Recent statistics with figure 4 certifies the companies' incentives to lead in the Georgian insurance market.

The insurance companies will examine claims with their reinsurer organisations in case of need, which is another good point of gaining more experience in assessing the cyber-incidents and improving the knowledge in the Georgian insurance market.

2.8.2 The share of cyber-insurance in the Georgian insurance market

The share of insurance packages in the Georgian insurance market formulate that (Figure 5) leading insurance types are health, property, road transport means (Casco), etc. There is no entry that specify a cyber-insurance, which emphasises, that the product is new in the Georgian insurance market. The facts that none of the companies give feedback regarding sold cyber-insurance policies' quantity assert that the product is on a very early stage of the implementation process. The insurance companies have sold some of the policies, but the number is so low, that does not make any sense to register as a separate product in statistical information conducted by "LELP Insurance State Supervision Service of Georgia".[109]

2.8.3 Low adoption and awareness

Firstly, low adoption is explained with little awareness of a cyber-insurance product in the Georgian market. The feedback from the **A3**'s representative strengthens the opinion

[108] "ALDAGI"'s online article. Available at: https://www.interpressnews.ge/ka/article/454804-kiberdazgveva-aldagis-unikaluri-shetavazeba-momxmarebels [Accessed: 07.04.2019] && UNISON online article. Available at: https://unison.ge/en/news/cyber-insurance [Accessed: 07.04.2019]

[109] LELP Insurance State Supervision Service of Georgia. Available at: http://insurance.gov.ge [Accessed: 07.04.2019]

that the knowledge is even low inside the insurance provider organisations, nothing to say regarding the demand side participants.

Cyber-insurance is not known for a broad audience since the Georgian cyber-insurance market is still young and not ready for such a product. The inquired insurance companies' representatives believe that in the country where the awareness is low of the MTPL[110] (the issue was framed during the interviews process for comparison purposes) product, it will be difficult to explain the need of a cyber-insurance.

Other insurance companies, who do not provide a cyber-insurance, have had pretty much the same answers, that the insurance market does not require a cyber-insurance, which can be asserted once again with low awareness, limited financial resources and unregulated laws regarding protecting the electronic data. The assertion can be strengthened by according to **A4**'s informant indication, that they stopped offering a product because of none existing demand.

2.8.4 Decision-making reasons (not) buying a cyber-insurance in banks

Considered, that the Georgian commercial banking sector is most developed rather than the other private area. The feedback got from the **B1,** and **B2** shows that the banks are only at the very beginning stage of assessing their enterprise risks and considering acquire the cyber-insurance packages for the future. **B1**'s informant told that according to his information currently in Georgia there are only one or two other banks, who already have brought cybercrime insurance packages.

The following aspects clarify the decision-making reasons in the banks no to take out a cyber-insurance: no regulations forcing to acquire a cyber-insurance, limited resources and low awareness on top management layers, the Georgian cybercrime practice and the experience.

[110] MTPL – Motor third party liability

Firstly, no regulations and must have directives acquiring a cyber-insurance negatively influence on protecting entities against cybercrime, as well as on increasing the knowledge and awareness following the common practices.

Secondly, according to the bank's informants, risk management is aware of cybercrime insurance and willing to implement it, though they disagree with top management layers, which might be explained because of limited resources and with the fact, that they have not yet experienced such case where the cyber-insurance would be useful.

Finally, the major influential factor considering taking out a cyber-insurance is the increased cybercrime cases in Georgian practice, especially in the banking sector. Recent cyber-attacks against TBC Bank are the bright examples, which give incentives to the banks to implement insurance packages against IT[111] crime. The informants admitted that market reality and experience indicate them to take appropriate measures into account. Increased cybercrime cases are the best incentives and motivation for the banks taking out a cyber-insurance against IT crime.

2.8.5 The information-sharing attitude of cyber-incidents

All the informants showed negative attitude toward cyber-incidents' information-sharing unless appropriate regulator obliges. Negative attitude has an unfavourable impact on increasing knowledge and awareness of a cyber-insurance product. Mainly, such an approach represents an obstacle on the way of understanding the need of the product, which eventually blocking implementation process of cyber-insurance and decreases its usage.

2.8.6 Rejecting the study of conceptual framework

According to received feedback, it's easy to reject the theoretical framework study ultimately for the case of Georgia. Firstly, the insurance companies do not have yet any

[111] IT- Information technology

claims for a cyber-insurance, nothing to say about the low awareness and usage of the product. Secondly, banks are only on their way of assessing their enterprise risks and considering implementing a cyber-insurance. The none existing claims on insurance companies' side, and not acquired cyber-insurance product with **B1**'s informant acknowledgement, that they prefer to buy a cyber-insurance policy from a more experienced foreign company rather from the local market, confirms, that nowadays in Georgia, the insurance industry and banking sector activities do not have any influence on per capita economic growth.

2.8.7 The reasons for the low use of cyber-insurance

There are following nine main reasons for the low use of cyber-insurance in Georgia.

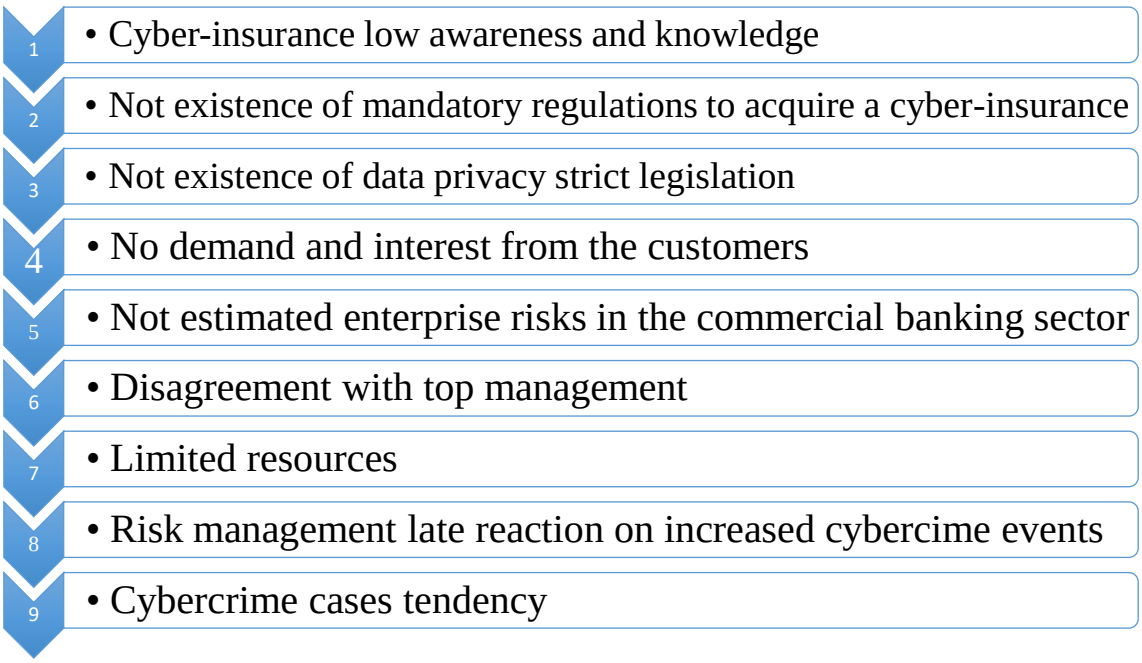


Figure 7. Reasons of cyber-insurance low use in Georgia.

Cyber-insurance low awareness and knowledge: are explained not much of the enthusiasm from the insurance companies' side to advertise the product to the broad audience. The low awareness and the knowledge on its behalf outline not existence of data privacy strict legislation and regulations since companies are not interested in

protection of information systems[112] unless cybercrime affects them. As on the individuals' level, the knowledge is much more unfortunate, since most of the people do not even know and can't understand the need of MTPL,[113] nothing to mention regarding cyber-insurance.

Not existence of data privacy legislation and regulations: do not promote incentives to protect a business from unexpected cyber threats, but it encourages saving resources and spending less on security measures. As from the customer's point of view, a none protected service does not seems to be very attractive, which at the end influences negatively on a company itself.

No demand and interest from the customers: are connected to the above defined two factors. Low awareness and the knowledge with none existing regulations and legislation alongside not experienced cyber-attacks on an organisation, does not invoke any interest in the company to acquire a cyber-insurance product.

Not estimated enterprise risks in the commercial banks: are the prerequisites to start considering the cyber-insurance implementation process. In the 21st-tech century, evaluating enterprise risks should be happening periodically to be up to date with new security standards.

Disagreement with top management: represents the starting point of much of the problems. Either risk management does not provide precisely with the necessary information to the top management regarding the necessity a cyber-insurance, either the company is already facing with other troubles, such are limited resources or so; hence they can't settle down to implement a risk transfer strategy as a risk management tool.

Limited resources: represents a common obstacle to many companies. If funds for the company are few and not affordable to buy a cyber-insurance, there is no wonder that the entity starts looking other solution(s) such are risk avoidance, retention or mitigation. When regulations and legislation do not oblige a company to acquire a cyber-insurance, and a company has not been a victim to the cyber-attacks, there is a little chance that a

[112] IoT – Internet of things

[113] MTPL – Motor third party liability. One of the outlined factor by insurance company informant.

company starts thinking to shrink its already few resources by transferring risks to a third party.

Risk management late reaction on increased cybercrime events: can be explained with the simple reason that the private banking sector is functioning with existing Georgian reality. It is in human nature to dismiss the possible dangers before the case has happened. Hence, they are not eager to see forward and take measures in advance following world-wide common practices to transfer financial losses caused by the cybercrime unless they have not faced the problems, or they are not on the edge of the cyber threats.

Cybercrime cases tendency: is the most significant influential factor in nowadays Georgian reality, which give incentives to the commercial banks to consider implementing a risk transfer strategy. The study shows that the private banks are reacting on scaled-up cyber incidents which are taking place more frequently recently and therefore willing to buy a cyber-insurance.

CHAPTER 3: RECOMMENDATIONS FOR IMPROVING THE USE OF CYBER-INSURANCE IN GEORGIA

3.1 Society initiative to increase cyber-insurance awareness

Generally, society is exposed to all kind of threats, including cyber. From the cybersecurity point of view, people can't be relied only on the government to be protected and supported by security measurements. The 21st high-tech century is continuous cyber siege bombarded with smart hackers and cyber criminals which numbers are tremendously increasing. Therefore, practice shows that all of us should take responsibility to defend ourselves. To achieve it the awareness and knowledge of the cyber threats should rise in society. This recommendation is also outlined in the book Solving Cyber Risk[114] (*Andrew Coburn, Eireann Leverett, Gordon Woo*) to strengthen the guidance, that the society should be awake and aware of modern cyber threats not to become victim of smart hackers.

Nowadays, in Georgia, the commercial banks are already providing with the necessary information to society to be warned regarding cyber threats and defend ways.[115] People should change their mindset feeling protected because behind them is the bank, and they should show an initiative to increase the awareness and knowledge not to become a victim of cybercrime.

Eventually, when cyber threats' awareness and knowledge is high in society, it will become evidence that the individuals start taking out the cyber-insurance policies as well to cover their private financial losses caused by cybercrime.

---

[114] SOLVING CYBER RISK PROTECTING YOUR COMPANY AND SOCIETY – ANDREW COBURN, EIREANN LEVERETT, GORDON WOO, pp 153 - 158

[115] My experience as being a customer to the commercial banks in Georgia. They provide the cyber threats information and defend ways on their official and social web pages, also in internet banks.

3.2 Cyber-insurance workshops

Cyber-insurance provider insurance companies should organise workshops regarding the necessity of cybercrime insurance to a broad audience, starting from their internal customers ending with any interested individuals. They should discuss, that in the 21st century no one is protected entirely from cyber threats and cybercrime might become vital for an organisation survival from bankruptcy in case of cyber-incidents.

Such meetings will help to increase the awareness and the knowledge of the product in the country. On the other hand, workshops give incentives to other insurance companies to provide a cyber-insurance, which eventually will be beneficial for product development. As the result of increased awareness, the use of a cyber-insurance should improve in Georgia.

3.3 Cybersecurity regulations and legislation

Countries with strict data regulations and legislation mainly are subject to higher fines in case of cybercrime. The higher expenses and financial losses are one of the main reasons for acquiring a cyber-insurance. Figure 8 below shows the world map of data privacy regulation.

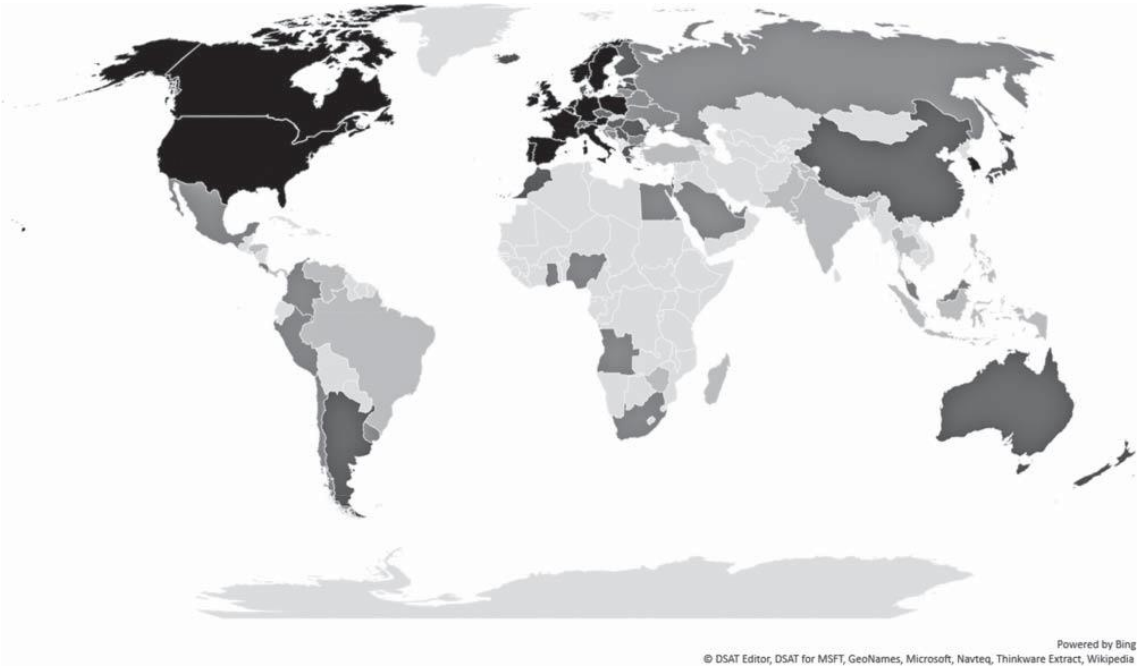


Figure 8. World map of data privacy regulation. In darken regions, there are more strict data privacy regulations. '**SOLVING CYBER RISK PROTECTING YOUR COMPANY AND SOCIETY – ANDREW COBURN, EIREANN LEVERETT, GORDON WOO, pp 182 – 205.**'

As for the case of Georgia, it's seen that there is no strict data privacy regulations and legislation. Nonetheless, Georgia already has a cybersecurity strategy, and there are defined principles of how to enhance cybersecurity operations, the government should implement legislation which will oblige companies to protect customers data more strictly and transparently. For example, replicating the GDPR[116] legislation, regarding customer's data strict protection will give incentives to organisations to care more on their client's confidential information and insure unexpected cyber incidents. Such regulations and fair of high fines will naturally influence on risk management strategies, and companies eventually consider taking out a cyber-insurance.

3.4 Cyber-incidents information sharing attitude

Another factor in improving the use of cyber-insurance product is the cyber-incidents information-sharing positive attitude. Information-sharing from a victim company will give its experience and practice to other companies. Organisations sharing each other's

[116] GDPR – General data protection regulation

expertise and the knowledge lead to a decrease in financial losses caused by cyber-attacks. One company's fault will indicate another organisation to increase their understanding and awareness against cyber threats and implement a cyber-insurance as a risk management tool.

3.5 Cyber-insurance alternative way

An alternative way of a cyber-insurance is a self-insurance. A company estimates it risks the likelihood of financial losses and managing the balance sheet. Reserves as much budget, as it will be enough to cover potential future shocks in case of cyber-attacks. However, estimating the risks and the likelihood of financial losses are quite tricky, hence still it is a better option to acquire a cyber-insurance instead.

Self-insurance is a solution for companies with limited resources that a company should take as much risk as it will be to handle in case of potential cybercrime.

3.6 Internal communication management

The study shows that communication between top and risk management should be improved. Risk management should explain common practices and the need for a cyber-insurance. Providing financial losses examples from global central banks should increase top management layers awareness.

That risk management should not be one step behind, but one step forward to ongoing cybercrime tendency in the country. Risk management should not be the passive foreseen possibility of cyber-attacks by looking at other companies' examples which are already victims of cybercrime.

3.7 Cyber-insurance and economic growth

The feedback got from the commercial banks indicate that they are estimating their enterprise risks to implement a cyber-insurance for the future, which is influenced mainly with cybercrime increased tendency in Georgia.

The conceptual framework study shows that cyber-insurance impact on reducing financial losses caused by cybercrime in commercial banks for the long-run eventually will influence on economic growth per capita. Therefore, implementing the product is not only beneficial for the company to insure cyber risks, but for the country's sustainable economic development.

CONCLUSION

Cyber-insurance product that is provided in the Georgian insurance market covers first-party and third-party losses with some other benefits including first response, communication costs, etc. The product is supplied for big companies, including commercial banks. The insurance companies are up for negotiations with clients to offer a package that is in need. Nonetheless that, the product has been created only for the reputation purposes, already two insurance companies provide it and the product is designed, which on its behalf is the deposit for cyber-insurance product development for the future.

The investigated insurance companies have not tried much to spread the knowledge and awareness of a cyber-insurance to a broad audience. They only used direct and email marketing with their already existing customers. They are interested in the product advertising publicly for the future though, as soon as they identify interest toward a cyber-insurance.

As for the demand side participants of cyber-insurance, it can be said that only a few of the organisations have insured their cyber risks. Customers are so few that they can't be separated and classified in the statistics on the Georgian insurance market. Therefore, a cyber-insurance does not have yet a dedicated register and market share in recent statistical information.

Since a cyber-insurance product is entirely reinsured by world's leading reinsurers and the insurance companies can handle massive cybercrime incidents, the primary target for the product from the insurance companies are financial institutions including commercial banks and other prominent organisations.

Georgian commercial banking sector practice shows, that they mostly following their own experience, unless they are not obliged to acquire a cyber-insurance. Disagreement with the top management layer buying the product policy might be another influential factor with the limited resources. Based on the conducted investigations, it is visible, that recently increased cybercrime tendency in Georgia gives incentives to the banks for analysing their enterprise risks and to acquire a cyber-insurance.

The investigation shows that at the very moment of writing this master's thesis there is still a growing cyber-insurance market in Georgia. The product is already well formed for the starting point, offered by two leading insurance companies who can provide coverage for the massive cybercrime incidents.

The study presents two main directions for further work. Firstly, it can be examined why the commercial banks do not show their enthusiasm contributing to the study, taking into an account, that the feedback gets from the informants are anonymous and will not be disclosed. And, secondly, since nowadays a cyber-insurance market is still young, will be helpful to repeat the research in several years after, compare the results, similarities and differences. When a cyber-insurance usage is reasonable, can be inspected the impact of the product on reducing cybercrime costs and reviewed again the above outlined conceptual framework model.

REFERENCES

[1] "Federal Bureau of Investigation Internet Crime Complaint Center (IC3)," [Online]. Available: https://www.ic3.gov/about/default.aspx. [Accessed 07 May 2019].

[2] T. Koulopoulos, "60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)," [Online]. Available: https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html. [Accessed 07 May 2019].

[3] Nino, "კიბერ დაზღვევა - პირველად საქართველოში უნისონისგან / Cyber-insurance - First time in Georgia by UNISON," [Online]. Available: https://unison.ge/en/news/cyber-insurance. [Accessed 13 February 2019].

[4] "National Cyber Security Index (NCSI)," [Online]. Available: https://ncsi.ega.ee/ncsi-index. [Accessed 13 February 2019].

[5] E. L. ANDREW COBURN, SOLVING CYBER RISK PROTECTING YOUR COMPANY AND SOCIETY.

[6] "The Rise and Rise of the Georgian Banking Sector," [Online]. Available: https://emerging-europe.com/georgia-2017/the-rise-and-rise-of-the-georgian-banking-sector/. [Accessed 22 April 2019].

[7] "Bank of Georgia (BOG)," [Online]. Available: https://bankofgeorgia.ge/en/home. [Accessed 22 April 2019].

[8] "TBC Bank Official Web Page," [Online]. Available: http://www.tbcbank.ge/web/en/personal-banking. [Accessed 22 April 2019].

[9] "Financial market's economic performance," [Online]. Available: https://www.frbsf.org/education/publications/doctor-econ/2005/january/financial-markets-economic-performance. [Accessed 14 February 2019].

[10] "G-20 countries," [Online]. Available: http://g20.org.tr/about-g20/g20-members. [Accessed 14 February 2019].

[11] M. B. A. M. N. J. H. H. A. G. Rudra P. Pradhan, "Is there a link between economic growth and insurance and banking sector activities in the G-20 countries?".

[12] "SEC – Securities and Exchange Commission," [Online]. Available: https://www.sec.gov/Article/whatwedo.html. [Accessed 28 February 2019].

[13] *Securities and Exchange Commission "CF Disclosure Guidance: Topic No.2—Cybersecurity",* 2011.

[14] *Securities and Exchange Commission "Commission Statement and Guidance on Public Company Cybersecurity Disclosures",* 2018.

[15] "LAW OF GEORGIA ON INSURANCE," [Online]. Available: http://insurance.gov.ge/getattachment/Legislation/Normative-Acts/Law_On_Insurance.pdf.aspx. [Accessed March 2019].

[16] “Insurance State Supervision Service of Georgia,” [Online]. Available: http://insurance.gov.ge/getattachment/Useful-Information/List-of-license-documents-eng.pdf.aspx. [Accessed March 2019].

[17] “THE CONSTITUTION OF GEORGIA,” [Online]. Available: http://www.parliament.ge/files/68_1944_951190_CONSTIT_27_12.06.pdf. [Accessed March 2019].

[18] “ORGANIC LAW OF GEORGIA ON THE NATIONAL BANK OF GEORGIA,” [Online]. Available: https://www.nbg.gov.ge/uploads/legalacts/fts/eng/on_the_national_bank_of_georgia.pdf. [Accessed March 2019].

[19] “Ministry of Internal Affairs,” [Online]. Available: https://police.ge/en/home. [Accessed 30 March 2019].

[20] “AI for everyday conversations,” [Online]. Available: https://otter.ai/about. [Accessed 31 March 2019].

[21] “ISIC - International Student Identity Card,” [Online]. Available: https://www.isic.org/about-us/. [Accessed 31 March 2019].

[22] “AIG,” [Online]. Available: https://www.aig.com/about-us. [Accessed 4 March 2019].

[23] “LELP Insurance State Supervision Service of Georgia,” [Online]. Available: http://insurance.gov.ge/. [Accessed 7 April 2019].

[24] “ALDAGI,” [Online]. Available: http://aldagi.ge/en. [Accessed April 2019].

[25] “UNISON,” [Online]. Available: https://unison.ge/en/about-us. [Accessed April 2019].

[26] “"ALDAGI"'s online article about cyber-insurance,” [Online]. Available: https://www.interpressnews.ge/ka/article/454804-kiberdazgveva-aldagis-unikaluri-shetavazeba-momxmarebels. [Accessed 7 April 2019].

[27] “Cyber-Insurance – “ALDAGI”’s unique offer to a customer,” 2017. [Online]. Available: https://www.interpressnews.ge/ka/article/454804-kiberdazgveva-aldagis-unikaluri-shetavazeba-momxmarebels. [Accessed 3 April 2019].

[28] “Cyber-Insurance - First time from UNISON in Georgia,” 2017. [Online]. Available: https://unison.ge/en/news/cyber-insurance. [Accessed 4 March 2019].

[29] “PSP Insurance,” [Online]. Available: http://ipsp.ge. [Accessed March 2019].

[30] “IMEDI L,” [Online]. Available: https://www.imedil.ge/en/about-company. [Accessed March 2019].

[31] “How to protect from cyber-attacks to minimize loses to a minimum,” 2018. [Online]. Available: https://on.ge/story/17193-%E1%83%90%E1%83%9A%E1%83%93%E1%83%90%E1%83%92%E1%83%98. [Accessed 3 April 2019].

[32] “Privacy Policy of “Otter.ai”,” [Online]. Available: https://otter.ai/privacy. [Accessed 31 March 2019].

[33] “Deputy of Minister of Internal Affairs comment on cybercrime on TBC,” 2019. [Online]. Available: https://news.ge/kibersheteva-tbcze. [Accessed 30 March 2019].

[34] “Cyberattack on TBC Bank,” 2018. [Online]. Available: https://www.bm.ge/ka/article/tbc-ze-kibersheteva-2018-wlis-16-ivliss-ganxorcielda---tbc-is-werilebi-gasajarovda/31094. [Accessed 30 March 2019].

[35] “Licensed insurance company register in Georgia,” [Online]. Available: http://insurance.gov.ge/Insurance-companies.aspx. [Accessed March 2019].

[36] F. B. o. Investigation, “Internet Crime Report,” 2018. [Online]. Available: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf.

[37] ““WannaCry” ransomware attack – Technical intelligence analysis,” 2017. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf. [Accessed 28 February 2019].

[38] K. M. Eisenhardt, “Building Theories from Case Study Research,” [Online]. Available: https://www.uio.no/studier/emner/matnat/ifi/INF5571/v15/timeplan/ar-docs/eisenhardt-1989.pdf. [Accessed 13 March 2019].

[39] R. K. Yin, “Case Study Research Design and Methods (Second Edition),” [Online]. Available: http://www.madeira-edu.pt/LinkClick.aspx?fileticket=Fgm4GJWVTRs%3D&tabid=3004. [Accessed 13 March 2019].

[40] “Critical Security Controls for Effective Cyber Defence,” [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf. [Accessed February 2019].

[41] A. S. a. F. Z. Pythagoras Petratos, “Cyber Insurance,” [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F978-3-319-06091-0_25-1.pdf. [Accessed 5 May 2019].

[42] “Cyber insurance – Statistics & Facts,” [Online]. Available: https://www.statista.com/topics/2445/cyber-insurance. [Accessed 14 February 2019].

[43] A. Bouveret, “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,” [Online]. Available: https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx. [Accessed 28 February 2019].

[44] E. L. K. C. W. Kopp, “Cyber Risk, Market Failures, and Financial Stability,” 2017. [Online]. Available: https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx. [Accessed March 2019].

[45] G. o. Georgia, “Cybersecurity Strategy of Georgia,” 2018. [Online]. Available: http://csbd.gov.ge/doc/Cybersecurity%20Strategy_eng.pdf. [Accessed 23 February 2019].

[46] “Frauds in banking industry,” [Online]. Available: https://financialregnews.com/banking-industry-suffered-2-2-billion-fraud-losses-2016. [Accessed May 2019].

[47] “GDP by Country 2019,” [Online]. Available: http://worldpopulationreview.com/countries/countries-by-gdp. [Accessed 14 February 2019].

[48] “Georgian Banking Sector Overview,” 2018. [Online]. Available: https://home.kpmg/ge/en/home/insights/2018/09/overview.html. [Accessed March 2019].

[49] I. O. f. Standardization, “Information technology Security techniques - Information security risk management,” 2011.

[50] M. E. a. J. W. Biener C, “Insurability of Cyber Risk: An Empirical Analysis,” *The Geneva Papers,* vol. 40, 2015.

[51] B. Schneier, “Insurance and the computer industry,” [Online]. Available: https://doi.org/10.1145/365181.365229. [Accessed 28 February 2019].

[52] R. S. d. G. David Niemeijer, “A conceptual framework for selecting environmental indicator sets,” [Online]. Available: https://doi.org/10.1016/j.ecolind.2006.11.012. [Accessed 11 March 2019].

[53] L. G. Ranjan Pal, “Analyzing Self-Defense Investments in Internet Security Under Cyber-Insurance Coverage,” 2010. [Online]. Available: https://doi.org/10.1109/ICDCS.2010.79. [Accessed 10 May 2019].

[54] “Commonality of risk assessment language in cyber insurance - Recommendations on cyber insurance study,” 2017. [Online]. Available: https://doi.org/10.2824/691163. [Accessed 28 February 2019].

[55] G. S. M. F. J. W. Nikhil Shetty, “Competitive Cyber-Insurance and Internet Security,” 2010. [Online]. Available: https://doi.org/10.1007/978-1-4419-6967-5_12. [Accessed 10 May 2019].

[56] J. B. Lelarge, “Cyber Insurance as an Incentive for Internet Security,” 2008. [Online]. Available: https://doi.org/10.1007/978-0-387-09762-6_13. [Accessed 10 May 2019].

[57] S. C. D. S. A. M. S. K. S. Arunabha Mukhopadhyay, “Cyber-risk decision models: To Insure IT or not?,” [Online]. Available: https://doi.org/10.1016/j.dss.2013.04.004. [Accessed 2 March 2019].

[58] G. o. Georgia, “Cybersecurity Strategy of Georgia,” 2018. [Online]. Available: http://csbd.gov.ge/doc/Cybersecurity%20Strategy_eng.pdf. [Accessed 23 February 2019].

[59] M. Butler, “Effective global regulation in capital markets Speech at the ICI Conference,” London, 2017.

[60] L. K. J. F. W. Jackson, “Evaluation Guidelines for Ecological Indicators. Environmental Protection Agency, Washington, DC,” 2000.

[61] “General Data Protection Regulation (GDPR),” [Online]. Available: https://gdpr-info.eu. [Accessed 3 April 2019].

[62] L. M. &. O. D. Gurgenidze L, “Georgia: from Planning to Hyperinflation,” p. 259–289, 1994.

[63] I. S. S. S. o. Georgia, “Insurance market statistics,” [Online]. Available: http://insurance.gov.ge/Statistics.aspx. [Accessed May 2019].

[64] P. K. Michael Payne, “Insuring the uninsurable: Is cyber insurance really worth its salt?,” [Online]. Available: https://intranet.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2017/michaelpayneisg.pdf. [Accessed 2 March 2019].

[65] K. K. L. V. Eneken Tikk, “INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS,” 2010. [Online]. Available: https://doi.org/10.1111/joes.12004. [Accessed 13 February 2019].

[66] “INTERNET CRIME REPORT,” 2018. [Online]. Available: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf. [Accessed May 2019].

[67] M. B. A. M. N. J. H. H. A. G. Rudra P. Pradhan, “Is there a link between economic growth and insurance and banking sector activities in the G-20 countries,” [Online]. Available: https://doi.org/10.1016/j.rfe.2017.02.002. [Accessed 14 February 2019].

[68] “List of active commercial banks in Georgia,” [Online]. Available: https://www.nbg.gov.ge/index.php?m=403&lng=eng. [Accessed March 2019].

[69] M. Bughulashvili, “Maka BughulashviliGlobal Economic Crisis: Is Georgia At Risk?,” [Online]. Available: https://journal.ibsu.edu.ge/index.php/ibsusj/article/view/106. [Accessed 14 February 2019].

[70] “Managing Organizational Security – Cyber-Insurance in IT Security Management,” 2007. [Online]. Available: https://doi.org/10.1109/MSP.2007.57. [Accessed 10 February 2019].

[71] G. S. Rainer Böhme, “Modeling Cyber-Insurance: Towards A Unifying Framework,” 2010. [Online]. Available: http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf. [Accessed 28 February 2019].

[72] G. K. Rainer Böhme, “Models and Measures for Correlation in Cyber-Insurance,” [Online]. Available: http://sec2013.crysys.hu/~mfelegyhazi/courses/EconSec/readings/09_BohmeK2005insurance_correlation.pdf. [Accessed 10 May 2019].

[73] “National Bank of Georgia (NBG),” [Online]. Available: https://www.nbg.gov.ge/index.php?m=130&lng=eng. [Accessed March 2019].

[74] S. C. f. S. a. International, “Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II,” 2014.

[75] “NOTPETYA TECHNICAL ANALYSIS,” [Online]. Available: https://gallery.logrhythm.com/threat-intelligence-reports/notpetya-technical-analysis-logrhythm-labs-threat-intelligence-report.pdf. [Accessed 28 February 2019].

[76] G. o. t. S. o. t. E. O. f. E. C.-o. a. Development, “OECD Core Set of Indicators for Environmental Performance Reviews: A Synthesis Report,” Paris, 1993.

[77] “Organization for Economic Cooperation and Development,” [Online]. Available: http://www.oecd.org/about. [Accessed March 2019].

[78] M. A. Starr, “QUALITATIVE AND MIXED-METHODS RESEARCH IN ECONOMICS: SURPRISING,” 2014. [Online]. Available: https://doi.org/10.1111/joes.12004. [Accessed 13 March 2019].

[79] “RECENT ECONOMIC DEVELOPMENTS – GEORGIA,” [Online]. Available: https://www.worldbank.org/en/country/georgia/overview#3. [Accessed 14 February 2019].

[80] T. Vissak, “Recommendations for Using the Case Study Method in Internation Business Research,” [Online]. Available: https://files.eric.ed.gov/fulltext/EJ875260.pdf. [Accessed 13 March 2019].

[81] “Registered insurance companies,” [Online]. Available: http://insurance.gov.ge/Insurance-companies.aspx?lang=en-US. [Accessed March 2019].

[82] “Short History of State Insurance Supervision Service Development,” [Online]. Available: http://insurance.gov.ge/About-Us.aspx?lang=en-US. [Accessed March 2019].

[83] S. Friedman, *Taking cyber risk management to the next level - Lessons learned from the front lines at financial institutions*, 2016.

[84] W. S. F. S. Martin Eling, “Ten Key Questions on Cyber Risk and Cyber Risk Insurance,” 2016. [Online]. Available: https://www.genevaassociation.org/media/954708/cyber-risk-10-key-questions.pdf. [Accessed 10 May 2019].

[85] P. Shakarian, “The 2008 Russian Cyber-Campaign Against Georgia,” 2011. [Online]. Available: https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia. [Accessed 8 May 2019].

[86] U. Franke, “The cyber insurance market in Sweden,” 2017. [Online]. Available: https://doi.org/10.1016/j.cose.2017.04.010. [Accessed 10 May 2019].

[87] J. F. &. J. N. David Amaghlobeli, “The Evolution of Commercial Banking in Georgia,” 2001. [Online]. Available: https://doi.org/10.1080/1463137032000058386. [Accessed March 2019].

[88] W. Y. J. P. K. Ruperto P. Majuca, “THE EVOLUTION OF CYBERINSURANCE,” [Online]. Available: https://arxiv.org/ftp/cs/papers/0601/0601020.pdf. [Accessed 28 February 2019].

[89] “What do we know about cyber risk and cyber risk insurance?,” [Online]. Available: https://doi.org/10.1108/JRF-09-2016-0122. [Accessed 28 February 2019].

[90] V. S. M. a. R. C. R. Tridib Bandyopadhyay, “Why IT managers don't go for cyber-insurance products,” 2009. [Online]. Available: https://doi.org/10.1145/1592761.1592780. [Accessed 10 May 2019].

[91] “Zero-Day exploit – cyber-attack that occurs on the same day a weakness is discovered in software,” [Online]. Available: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit. [Accessed 2 March 2019].

[92] A. G. Vladimer Svanadze, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები - ვლადიმერ სვანაძე, ანდრია გოცირიძე / Main players of cyberspace, cyber-security politics, strategy and challenges.

[93] G. o. Georgia, “საქართველოს ეროვნული უსაფრთხოების კონცეფცია - National security concept of Georgia,” [Online]. Available: https://mod.gov.ge/uploads/2018/pdf/NSC-GEO.pdf. [Accessed 13 February 2019].

Appendix 1 – Interview Questions for Insurance Companies

Introduction

1. What are your background and the position in the company?
2. How long have you been working in the insurance industry? In the company?
3. Is your insurance company reinsured?
4. Generally, how often does the company analyse customer's demands on the Georgian insurance market?
    a. How is determined analyses initiative?
        i. Is the process repetitive within some time interval?
5. Does your company provide a cyber-insurance product?
    a. If not:
        i. Have you analysed the demands of cyber-insurance product on Georgian market? If not, why?
            1. Do the analysis results seem not beneficial for the company? Why?
        ii. Generally, does the company try to increase awareness in society/organisations of the insurance products on the market?
            1. How the company does it?
            2. Has the company tried the same for a cyber-insurance product?
        iii. What are other reasons not providing the product?
    b. Are you considering providing a cyber-insurance product for near the future and when?

6. When did the company start selling cyber-insurance policies?
    a. On the Georgian market?
    b. On abroad (if any)?
7. In your opinion, to what degree is a cyber-insurance market in Georgia competitive?

Customers

8. Approximately how many customers have brought cyber-insurance policy from the company?
9. Based on what criterion does your company concentrate on selling a cyber-insurance product to customers (business sectors)?
    a. Business-specific cyber risk profiles?
    b. Lower/medium/higher premiums?
10. Mostly to what kind of customers (business sectors) does your company provide a cyber-insurance product?
    a. Do you provide the product to the banking sector in Georgia or any other financial institutions?
        i. If not, how do you think what are the reasons not providing?
11. How do you attract the cyber-insurance product customers?
    a. What are the ways you have done or willing to do to increase the knowledge and the awareness of the product on the Georgian market?
    b. How do you think, is the product know-how for the Georgian market?
    c. Is the awareness of the product low/medium/high on the Georgian market?

Product characterisation

12. Is cyber-insurance product providing more difficult compared to other products which your company offers?

    a. What are the difficulties? Maybe the estimation of risks and therefore calculating premiums?

13. Is cyber-insurance product more profitable compared to other products which your company provides?

14. What kind of packages do you provide for cyber-insurance product?

    a. What type of cyber incidents do your packages cover?

    b. Is there a particular type of incidents the company does not provide coverage?

    c. How do you determine the size of coverage?

15. What does the process of underwriting look like in your company for cyber-insurance product?

    a. How do you think, to what degree a candidate customer provides private information for assessing the cyber risks?

    b. How do you determine if the candidate customer cyber risk profile is acceptable or not?

    c. Mainly what are the reasons declining candidate customers for providing a cyber-insurance product?

    d. Do you set any requirements or regulations for the customers to provide a cyber-insurance product?

Claims & Information Sharing

16. Can you say approximately how many cyber-insurance claims have you received so far from the Georgian market?

    a. How many of them approved/declined?

b. What type of cyber incidents leading in claims?

c. Can you say if the company had such an approved claim which coverage was helpful for a customer not to go on bankruptcy?

d. After the claim is being approved, do you provide determined coverage or is it rechecked and recalculated?

    i. If so, can you provide reasoning for it?

17. What is the information sharing attitude from cyber-insurance customers regarding detected cyber incidents?

    a. How do you think, do the customers share such cyber incidents information for which they don't ask for the claim?

    b. Do customers willing to report claiming cyber incidents to appropriate governmental entities?

    c. Do you share cyber incidents information to other entities?

18. Can you provide additional information regarding the impact of cyber-insurance on reducing cybercrime costs in Georgia?

    a. Based on the company's statistical information and the knowledge, has cyber-insurance reduced cybercrime costs on Georgian market?

19. Thank you for the interview. Feel free to provide (if any) an additional related information/comments regarding a cyber-insurance product.

Appendix 2 – Interview Questions for Commercial Banks

Introduction

1. What are your background and the position in the company?
2. How long have you been working in the financial sector? In the bank?
3. Do you agree that in real-world security only can get through the insurance industry?
4. Which risk management strategies does the bank follow?
    a. Risk Avoidance
    b. Risk Retention
    c. Risk Mitigation
    d. Risk Transfer
5. Does the bank have a dedicated cybersecurity department?
    a. If not, can you explain why?
6. Does the bank hold cyber-insurance policy?

Bank holds a cyber-insurance policy

1. How long has the bank taken out a cyber-insurance policy?
2. Does the bank have a cyber-insurance policy from the Georgian insurance market?
    a. If not, can you provide reasoning on why choosing a foreign insurance company over Georgian one?
3. Does the bank have internal IT related security directives?

a. If yes, is it a must-have directive holding a cyber-insurance policy?

    i. If yes, can you provide more information on how and why did it happen to set it as a must-have the requirement?

4. Are there any obligations towards governmental regulations regarding IT security?

    a. If yes, does it include holding a cyber-insurance policy?

5. Can you say approximately how long time did it take for the bank to consider a cyber-insurance product as a mean of protection from cyber threats until it got acquired?

6. What can you say about the cyber-insurance product acquisition process?

    a. People of what position were involved internally from the bank into the operation?

        i. Was the cybersecurity department (if any) included?

        ii. Did the bank hire an insurance broker and was the effort useful?

    b. Was the decision for taking out a cyber-insurance based on:

        i. Risk assessment and managing enterprise risks?

        ii. Actual the experienced cyber incidents (if any)?

        iii. Cybersecurity department (if any) or specific individual/group suggestion?

        iv. Banking internal security regulations?

        v. Governmental or NBG regulations and legislation?

        vi. Worldwide common standards?

    c. Did the insurance provider company set requirements and obligations to the bank before taking the liability of the coverage?

i. If yes, what kind of requirements have been set?

1. Did it require technical or managemental changes?

2. Was it connected to additional resources?

d. How would you estimate, was it a complicated process finding a proper insurance company for the product?

i. Do you think that the bank evaluated decent coverage options for the product?

ii. Does the bank consider re-validate the product coverage options shortly and why?

7. What additional factors can you emphasize which were influential in acquiring a cyber-insurance policy?

8. How do you think, what is the impact of cyber-insurance product on the way how cybersecurity measures are taken into consideration in the bank?

9. What kind of cyber-insurance package(s) does the bank hold?

a. What types of cyber incidents does the cyber-insurance cover?

10. How do you think, does the cyber-insurance package covers risks which are essential for the bank or there are still the gaps between the needs and the coverage?

11. Can you say if cyber incidents have been detected and the cyber-insurance was useful covering the losses?

12. Overall based on experience, are you satisfied with the cyber-insurance product?

13. What is the attitude of cyber incidents sharing and reporting with the insurance company, governmental entities and with customers?

a. With other financial institutions?

b. Can you remember such a case, when cyber incidents have happened, but the bank did not require the claim from the insurance company and dealt with them internally?

    i. If yes, can you explain why?

c. How do you think, will such a reporting system avoid and reduce damage caused by cybercrime incidents?

14. Thank you for the interview. Feel free to provide (if any) an additional related information/comments regarding the cyber-insurance product.

Bank does not hold a cyber-insurance policy

1. Does the risk management department is aware of cyber-insurance product and what coverages are available on the insurance market?

2. Do you think that the bank already has another type of insurance covering cyber-incidents implicitly?

    a. If yes, can you tell what kind of product it is?

3. How do you think what are the reasons, that the bank has not taken out a cyber-insurance product?

    a. When was the last time risk assessment has happened?

        i. Was the cybersecurity department (if any) included in the process?

        ii. People of what position were participated in the process?

    b. In your opinion, to what degree is estimated cyber risk profile for the bank?

    c. How do you think, recent successful cyber-attacks on central banks all over the world are not evident enough and facts to start considering a cyber-insurance product to secure devastating financial losses?

d. In your opinion, what are the problematic aspects of the bank acquiring a cyber-insurance policy?

4. Don’t you consider that holding a cyber-insurance policy will increase the trustworthiness of the bank customers, therefore promoting the banking business?

5. Does the bank consider acquiring a cyber-insurance policy for the future?

    a. If yes, can you provide reasoning?

        i. Based on what factors does the initiative come?

    b. If yes, does it mean that the bank has been slow to implement world-wide common standards and practices for the case of cyber-insurance?

    c. How do you think, would it be a good idea setting the must-having requirement internally in the bank holding a cyber-insurance policy?

6. Can you point out additional influential (beneficial) factors in acquiring a cyber-insurance policy?

7. What do you think, what are the main cyber risks relevant to the bank?

    a. How do you think, for what type of cyber incidents should be provided with a coverage?

8. How does the bank at the very moment deals with unexpected cyber threats?

    a. Who is involved in dealing with cyber-attacks?

    b. Does the bank follow world-wide common standards and practices, frameworks?

    c. Does the bank has implemented a management system for cybersecurity?

9. Are you satisfied and confident that the current management ways dealing with cyber risks are sophisticated?

    a. Does the bank regularly process penetration testing? When was the last time has it happened?

10. Can you say if the bank has identified unexpected cyber-incidents?
    a. If yes:
        i. To what degree was it harmful?
        ii. Has the bank reported and shared the cyber-incidents to appropriate governmental entities or other institutions, customers?
11. How do you think, has the bank came across to such a cybercrime where cyber-insurance would be useful?
12. How do you think, if the bank has taken out a cyber-insurance policy, how would it influence on cybersecurity operations? Would it be influential on the ways you are dealing with cyber threats nowadays?
13. What is the attitude sharing and reporting detected cyber-incidents with governmental entities and with customers?
    a. With other financial institutions?
    b. How do you think, will such a reporting system avoid and reduce damage caused by cybercrime incidents?
14. Thank you for the interview. Feel free to provide (if any) an additional related information/comments regarding the cyber-insurance product.

Appendix 3

Generic request to the insurance companies

To whom it may concern,

I am a cybersecurity student at Tallinn University of Technology and conducting the research regarding cyber-insurance product in Georgia. I'd like having an interview with your company's representative for the questions attached below. Face to face interview is preferred, via Skype is also fine though. However, if the meeting could not be organised, in such case, please provide answers via word document directly.

The goal of the research is to summarise knowledge and the experience of the cyber-insurance product on the Georgian market (mainly answering the question, ***what is the usage of cyber-insurance product on the Georgian insurance market****). Please contribute to the research and contact me as soon as possible when you have time for the interview. Thank you for your feedback preliminary and looking forward to your answer.*

Contact info:
Tel: ...
Skype: ...
Email: ...

NB. Interview questions are semi-structured, meaning that interviewee isn't limited providing any relevant information or even skip the inquiry in case of need. Interview in English will be appreciated.

Yours faithfully,

Tornike Nanobashvili

Appendix 4

Generic request to the banks

To whom it may concern,

I am a cybersecurity student at Tallinn University of Technology and conducting the research regarding cyber-insurance product in Georgia. I'd like having an interview with your company's representative for the questions attached below. Face to face interview is preferred, via Skype is also fine though. However, if the meeting could not be organised, in such case, please provide answers via word document directly.

The objective of the research is to summarise knowledge and the experience of the cyber-insurance product in Georgia (mainly answering the questions, ***what is the usage of cyber-insurance product on the Georgian insurance market****,* ***How are determined the decision-making reasons to acquire or not a cyber-insurance policy as a financial risk transfer strategy on the Georgian commercial banking sector****). Therefore, the goal of the study is getting the general knowledge of the commercial banking sector, how far the country went from recent cyber-attacks (since 2008) to implement cyber-insurance product as a risk management tool.*

Please contribute to the research and contact me as soon as possible when you have time for the interview. Thank you for your feedback preliminary and looking forward to your answer.

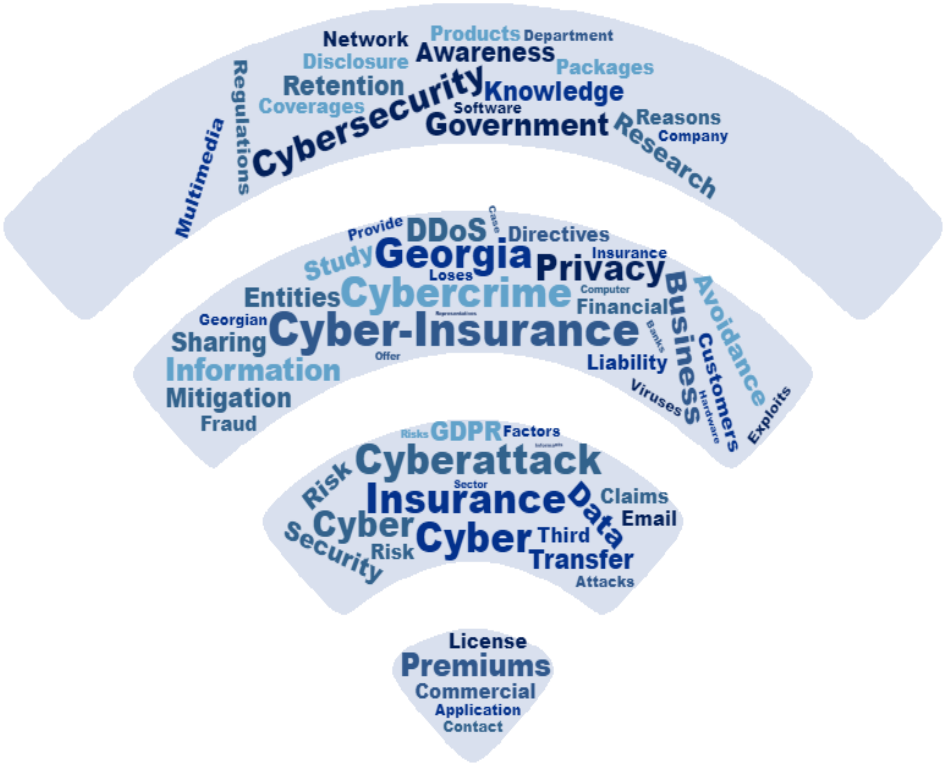
Contact info:
Tel: ...
Skype: ...
Email: ...

NB. Interview questions are semi-structured, meaning that interviewee isn't limited providing any relevant information or even skip the inquiry in case of need. Interview in English will be appreciated.

Yours faithfully,

Tornike Nanobashvili

Appendix 5 – Interview Word Cloud



Source: Based on conducted interviews, generated by https://wordclouds.com