DOI: 10.19192/wsfip.sj2.2020.2 ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

Cyber Insurance – Effective Mechanism for Protection against Cyber Threat

Nana Shonia[1], Tamila Khurtsidze [2] Zurab Mushkudiani [3]

[1]Department of Business Administration of Akaki Tsereteli State University
Georgia

[2] Department of Law of Akaki Tsereteli State University, Georgia
Georgia

[2] Department of Logistics of Batumi Navigation Teaching University, Georgia
Georgia

Abstract— **Cyber insurance is a rapidly developing area which draws more and more attention of practitioners and researchers. Insurance, an alternative way to deal with residual risks, was only recently applied to the cyber world. The immature cyber insurance market faces a number of unique challenges on the way of its development. In this paper we summarize the basic knowledge about cyber insurance available so far from both market and scientific perspectives. We provide a common background explaining basic terms and formalization of the area. We discuss the issues which make this type of insurance unique and show how different technologies are affected by these issues. We compare the available scientific approaches to analysis of cyber insurance market and summarize their findings with a common view. Finally, we propose directions for further advances in the research on cyber insurance.**

Index Terms— cyber-crime, insurance, digital economy, cyber risk, Technology Act.

I. INTRODUCTION

In recent years, there has been a growing interest to cyber risk and it is considered among the most challenging issues to deal with, as cyber risk could lead to serious impact on businesses and societies (Betterley, 2012) The expansion of information technology in business and in everyday reality through the spread of social networks, mobile devices, wireless technologies and cloud services has led to increased vulnerability (Johnson, 2014). Many companies are starting to consider cyber security as a large business risk and, as a consequence, they are looking for methods to ensure the continuity of financial operations in case of cyber-attacks. In parallel with the development of telecommunication and digital technologies, the number of cyber risks increased considerably in the 21st century (Airmic, 2012). Online fraud, unauthorized access to the computer system, unauthorized use of the computer system and data, etc. causes serious damage to the targets of the cyber-attack. In 2018 a number of facts were reported in different countries, where cyber criminals enter the systems of various companies, stop them, demand a huge ransom or block their operational systems, which is a major challenge to the world.

Insurance Premium Cyber insurance policies are often described as costly and far from fairly priced.68 There are at least four reasons for this: (1) the novelty of the product and thus the small size of risk pools; (2) the novelty of the product and thus the small number of market participants (limited availability); (3) the novelty of the product and limited data in regard thereto, making large risk loadings necessary, and (4) significant information asymmetries that require costly state verification and upfront risk assessment. According to Betterley, premiums for cyber insurance are currently high, especially for small and medium-sized companies, but relatively moderate considering the large uncertainties involved. Shackelford expects premium prices to decline with expanding and more competitive markets. This expectation is supported by recent market developments in the United States where new players entering the market induced slight premium decreases. Consumers of cyber insurance, according to the Ponemon study, confirm that cyber insurance premiums are not exceptionally high. In a survey of 638 cyber risk specialists in U.S. firms, 62% considered premiums to be "fair"; only 29% indicated that premiums are too high (Bradford, 2015). Compared to traditional property/liability insurance, however, there are additional costs associated with cyber insurance that must be covered. For example, there may be high upfront costs for assessing company risk (e.g., network security). Insurers demand those assessments and often additional information about past incidents before they will even offer a policy. Acquisition of that information can be a resource-consuming task. The upfront assessment, however, may have positive and

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 24, No 2 (2020), 6 pages
DOI: 10.19192/wsfip.sj2.2020.2
Received: 08.06.2020; Accepted: 24.06.2020

Regular research paper: Published 06.2020
Corresponding author's e-mail: z.mushkudiani@bntu.edu.ge

valuable side-effects in that it may increase company awareness of cyber risk, potentially increasing self-protective efforts. Indeed, the consulting and risk assessment services that insurance companies provide to firms seem to be a central driver of product value. One of the important economic functions of insurance is to put a price tag on risk and to set incentives for risk-appropriate behavior. The bottom line of the studies addressing premium adequacy for cyber risk is that cyber insurance premiums can be considered moderate in general; however, they are rather high for small and medium-sized corporations. Trends observed in recent years, however, indicate a decrease of premiums once the market expands and gains experience with cyber losses. (7) Cover Limits Cyber risk policies typically cover a maximum loss, but actual coverage limits vary. If we assume a US$ 50 million coverage limit, which is the maximum regular coverage we found for Swiss insurers, 92% of the cases in our data sample would be covered completely by the policy (Christian 2014). Whether this amount is acceptable depends on the risk preferences and cyber risk exposure of the individual policyholder. An increase in coverage should be negotiable, but will result in higher premiums. Policies typically contain several exclusions, e.g., self-inflicted loss, accessing unsecure websites, espionage, and terrorism. Additionally, there might be other indirect effects of cyber losses that cannot be measured and thus are not covered. An example is reputational loss, although some policies do include this type of loss in the coverage. For example, Gatzlaff and McCullough note that insurance often does not cover a large portion of data breach-related costs, such as losses to reputation and the impact on stock prices; also losses related to trade secrets and propriety information often are not covered. Another severe problem regarding cover limits is policy complexity. There are a large number of exclusions and the nature of cyber risk is very dynamic so that for the seller and the buyer, there is uncertainty about what the cyber policy actually covers. ENISA notes the lack of clarity as to coverage as one reason companies do not buy cyber insurance; it also notes that many companies believe that their existing property/liability policies are sufficient to cover cyber risks (Baranoff 2009).

Cyber-attacks have become especially worthy of note in case of companies storing a large amount of information electronically. An example of this is the National Health Service (NHS) of England, which experienced the cyber hell last summer. Hackers stole the personal data of Yahoo users in 2012, 2013 and 2014, and in 2008 the computers of the US armed forces were hacked.

Cyber risks, that is, loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality, are among the biggest new threats facing businesses and consumers. Cyber security risks are crucial as consumer, financial, and health information are increasingly stored in electronic form (Böhme 2010). Hackers, malware, viruses, tracking software, wiretapping, eavesdropping, rob calls, and solicitation lead to identity theft and compromised personal, financial, and health information. These breaches affect virtually every major industry, including, but not limited to, financial services, health care, government, entertainment, online gaming, retail, law, insurance, social networking, and credit card processing. As people become more reliant on electronic communication and organizations collect and maintain more information about their consumers, the opportunity for bad actors to cause problems for organizations and the public is growing exponentially. The number of data breaches tracked by the Identity Theft Resource Center (ITRC) in 2015 was 781, the second highest year on record since the ITRC began tracking breaches in 2005 (ITRC 2016). The Ponemon Institute, an independent research organization on privacy, data protection, and information security policy, notes that 75 percent of organizations surveyed experienced data loss or breach since 2014 (Ponemon Institute 2016). The Office of Civil Rights indicated that 112 million health-care-related records were lost, stolen, or inappropriately disclosed via data breaches in 2015. According to recent reports, the average cost of a data breach event for an organization is between 3 and 7 million dollars. In addition to financial and public relations damage, data breach events often threaten an organization's survival. Organizations also face compliance hurdles as they navigate between various, sometimes overlapping, federal and state laws and regulations concerning the collection and use of personal data. 2 The proliferation of security breaches in the last five years has resulted in an expansion of privacy laws, regulations, and industry guidelines. The increased flow of data across state boundaries, coupled with the increased enactment of data-protection-related statutes, creates significant challenges (Ehrlich 1972) for organizations operating at a national level to comply with the state and federal legal requirements. Even when there is no evidence that compromised data were used or otherwise disseminated, companies are still potentially subject to notification requirements, resulting in significant costs. Forty-seven states have notification statutes that require prompt notice of data breaches to those affected and to the state attorney general. Moreover, many statutes impose a significant daily fine for late notice or a private right of action for failure to comply. Finally, as the number of data breaches grows, so does the number of individuals pursuing legal action to remedy their injuries. Despite legal, reputational, financial, and survival threats, prevailing research suggests that private organizations are not significantly changing their behavior. Although many organizations do have formal policies in place, the majority of organizations do not believe they are sufficiently prepared for a data breach, have not devoted adequate money, training, and resources to protect consumers' electronic and paper-based information from data breaches, and fail to perform adequate risk assessments. In fact, because complying with multiple security frameworks is difficult, time consuming, and expensive, many organizations express "compliance fatigue". Recognizing this under preparation and under compliance gap, the insurance field stepped in during the last decade and began offering cyber insurance. Cyber insurance is insurance designed to provide both first-party loss and third-party liability coverage for data breach events, privacy violations, and cyber-attacks. Although there is variation in the types of policies being

offered, insurers offering cyber insurance provide some risk shifting for the costs associated with having to respond, investigate, defend, and mitigate against the consequences surrounding a cyber-attack. Compared to other lines of insurance, cyber insurance is in its infancy (Martinelli 2016). Therefore, there is limited data on how competitive the cyber market (Godinho 2013) is. However, we do know the cyber insurance market is growing rapidly as organizations become more aware of its potential usefulness. Whereas most companies did not have cyber insurance a decade ago, one in three organizations now has insurance specifically protecting against cyber and data theft losses.4 The insurance industry's most recent reports issued in 2015, indicate that 120 insurance groups are writing cyber insurance in the United States, totaling approximately $1 billion in direct written premiums with a loss ratio of 65 percent (Business Wire 2016).5 Recent estimates suggest that the global insurance market collected approximately $2 billion in cyber insurance premiums and that this will rise by a magnitude of three to five times by 2020 (Business Wire 2016). Cyber insurance, therefore, is one of the biggest areas of growth among insurers, and organizations, in turn, are increasingly purchasing cyber insurance to deal with these new risks.

Despite the increased attention on data theft and cyber insurance, there has been little research directed toward the role that insurance and, in particular, insurance institutions play in constructing the meaning of compliance with privacy laws and dealing with data breach. Drawing from participant observation and ethnographic interviews at cyber insurance conferences across the country, in addition to content analysis of cyber insurance policies, loss prevention manuals, cyber insurance risk management services, and webinars, my data suggest that insurance companies and institutions, through cyber insurance, go well beyond simply pooling and transferring an insured's risk to an insurance company or providing defense and indemnification services to an insured; rather, my data suggest that cyber insurers are also acting as compliance managers. By offering a series of risk management services developed within the insurance field, insurance institutions actively shape the way organizations' various departments tasked with dealing with data breach, such as in-house counsel, information technology, compliance, public relations (Gladishevskaya 2017), and other organizational units, respond to data breaches. Cyber insurance provides a pathway for insurance institutions to act as external compliance overseers and managers of organizational behavior with respect to data theft.

The developed countries of the world have to constantly take radical steps to make changes to the legal acts against cyber-crime. For instance, in the United States, there were regular legislative amendments related to cyber-crime. A new stage of legislative amendments started at the beginning of XXI century, which led to the introduction of the new law "Patriot Act" in October, 2001. The terrorist attacks of September 11 accelerated its preparation. The Act has expanded the authority of the Federal Bureau of Investigation in the area of electronic surveillance and eavesdropping. Pursuant to Article 814 of the Act, an amendment was made to Article 1030 (dealing with separate computer crimes) of Title 18 of the collection of laws (Pal 2017). As a consequence of the amendment the maximum limit of punishment for computer crime has been increased (the first crime – 10 years' imprisonment; a repeated crime – 20 years' imprisonment).

II. THE THEORY OF CYBER INSURANCE

With few exceptions, the academic cyber insurance literature consists of strictly theoretical papers that examine the viability of cyber insurance markets (Heal, 2003). Overall, this body of literature examines the incentives for firms to purchase insurance (demand side), the incentives for insurers to provide contracts (supply side), and the conditions necessary in order for a market to exist. The inevitable tension for firms, as many identify, is whether to invest in ex ante security controls in order to reduce the probability of loss, or to transfer the risk (cost) to an insurer. As the collective research describes, the defining characteristics of cyber insurance are interdependent security, correlated failure, and information asymmetry. Some of these properties are common to all insurance markets, while others -- and their combined effects -- are unique to the risks of networked computing systems and cyber insurance (Schutzer, 2015). First, interdependent security reflects the degree to which the security of one computer network is affected by the compromise of another system (the breached system is said to impose a negative externality on the victim). For example, the security of the DCA airport in Washington, D.C. may be compromised if luggage from SFO is not properly screened (Marsh 2013). Second, correlated failure (also known as systemic risk), is the systematic failure of multiple, disparate systems due to a single event. Correlated failures may occur in multiple ways, (Morgan 2015) such as from a single source (e.g. a criminal group attacking many businesses), failure of a single IT system upon which many businesses operate (e.g. cloud provider or virtualization data center), or compromise of many devices due to a common vulnerability or exploit (e.g. a distributed denial of service attack). (Notice the loss is further amplified by interdependent security.) Finally, information asymmetry in the context of insurance reflects the familiar moral hazard and adverse selection problems (i.e. companies behaving more risky when fully protected from loss; and insurance carriers not being able to differentiate between high and low risk clients).

III. RESEARCH METHODOLOGY

The goal of this research is to explore and describe the three main components of cyber insurance policies: coverage, applications, and rate schedules. In order conduct this analysis we conducted a directed content methodology which enables us to identify and categorize themes and concepts, and derive meaning and insights across policies

Germany started discussing legislative amendments in 2007. The legislation of Germany, unlike that of many other countries, did not impose the criminal liability for unauthorized

access to a computer or network. This behaviour was punishable only when it led to obtaining information, which needed to be changed according to Marco Gercke, an expert in the European Council. Marco Gercke deemed it as a fault and argued that unauthorized access to a computer system was to be punishable regardless of whether it led to any consequences or not. M. Gercke's recommendation was not considered in 2007. However, in March, 2009 he managed to have his point of view reflected in the German Criminal Code.

The United Kingdom ratified the Convention on Cybercrime on May 25, 2011, thus avoiding public criticism. The criticism was based on imposing the responsibility for the security of the computer system on Internet users. They were obliged to protect their own computer systems.

In Italy the Convention on Cybercrime came into force on October 1, 2008. However, since 1993 the Italian legislation has introduced punishment for unauthorized access to computer systems, computer fraud, improvement of computer data transmission, etc. A new regulation in the Italian Criminal Code, which deals with computer fraud, is especially interesting. It involves illegal use of an electronic signature through which the criminals receive illegal income for themselves or another person. The article is appealing because its subject can only be a person entitled to use an electronic signature. An electronic signature is known to have become more common throughout the world recently.

Pursuant to Article 635-B of the Italian Criminal Code, deterring the operation of a computer or computer system shall be punishable. Criminal liability is introduced for a person who has prepared or spread a device or computer program ensuring unauthorized access to a computer system.

An amendment was made to the Russian Criminal Code on December 7, 2011. As a result, Articles - 272, 273 and 274-3 were changed.

Pursuant to Article 272, it is punishable to illegally gain access to the computer information protected by law, if this act causes the destruction, blocking, modification or copying of computer information. The second part of the article includes aggravating circumstances: the action (included in the first part) taken for mercenary purposes or if the action has caused significant damage. The "significant damage" is defined as a loss which exceeds one million rubles.

Part 3 of Article 272 further aggravates the liability for the crime included in the first and second parts committed by a group or by using an official position. The fourth part defines the liability for the offense envisaged by Parts 1, 2 and 3 of Article 272 if it has dire consequences or there was a risk for such consequences.

The note of the same article defines the concept of computer information: "computer information" is the data presented in the form of an electronic signal regardless of the form of its storage, processing and transmission." This explanation does not correspond to the definition included in the convention, which demonstrates a narrow approach of the Russian legislation and it is incomplete since the object of protection of the Code is "computer information" instead of "computer system".

IV. THE WAYS OF FIGHTING CYBERCRIME IN GEORGIA

The question is - how does Georgia fight cybercrime and what is considered to be cybercrime?

The issue of cybercrime and cyber security has been particularly significant in Georgia since the events of 2008 when massive cyber-attacks were carried out against governmental and non-governmental online resources.

According to the data of the Ministry of Internal Affairs of Georgia, the number of the cases of cybercrime registered in Georgia increased by 151% in January-November of 2018 compared to the data of 2017. The number of the opened cases has decreased by three times and totals 8.75%. According to the crime statistics, 1051 cases of this type of crime were revealed throughout 11 months of the year and only 92 of them have been opened. This means that more than 90% of this type of crime was not opened last year. The sharp increase in the crime of this category indicates the necessity for the public to be more concerned about its own cyber security.

Pursuant to the Criminal Code of Georgia, cybercrime is an illegal act which includes one of the components of Articles 284, 285 and 286 of the Code, and not any unlawful act committed by using a computer system. For instance, unauthorized access to a computer system (284), unauthorized distribution of the password or access code required for access to a computer system (285), unauthorized damage to computer data (286), etc. Furthermore, there may be a combination of offences (articles), more specifically, unauthorized access to a computer system and subsequent secret acquisition of another person's movable thing (Articles 284 and 177 of the Criminal Code).

In addition, the Prosecutor's Office of Georgia developed a strategy of action to combat cybercrime in 2017-2021. The Law on "Information Security" was introduced, providing general standards for information security for public and private sectors. An office for combating cybercrime has been set up in the Central Criminal Police Department of the Ministry of Internal Affairs. The office is responsible for detection, suppression and prevention of illegal actions committed in the cyber space.

Apart from this, the LEPL Data Exchange Agency has developed general guidelines - a combination of practical rules for safe use of online resources. These guidelines include SPAM, FISHING, home Wi-Fi network security, MALWARE, BOTNET, e-mail and security.

As for the main regulatory international document of cyber-crime - the 2001 Convention of the European Council on Cybercrime, Georgia ratified it in 2012.

While studying the issue it became obvious that a guaranteed defense mechanism against this immensely dangerous crime does not exist in the world. However, there is one way which should function in parallel with the legal acts. This is cyber insurance - a type of insurance products, which provides compensation for the damage from hacker attacks. If a company's system is damaged by a cyber-attack and if it is not insured, the compensation by the founders may even lead to bankruptcy. Therefore, businessmen need to pay more attention to cyber insurance. Cyber insurance is a product

which makes the activities of companies and public sector as well as the rights of users far more secure.

Cyber insurance involves several stages and is actually oriented to the insurance of any risk. This can be hacker attacks as well as accidental damage and administrative or operational errors. For example, if computers or systems of a company are physically damaged or destroyed so that it is impossible to read digital data in them, cyber insurance provides compensation for the damages.

Cyber insurance has very wide coverage. First of all, it covers an error of an employee of the organization, and blocking or misusing the system. It is important that not only the entrance of third parties, but also the errors of the company's employees are insured. The insurance of this type covers electronic systems, as well as hardware, servers, computers, etc. The damage caused by the changes of the electric power is also covered.

The second component covered by the insurance is entering incorrect information or taking information from the company by an employee, i.e. errors made by the administrative and operational personnel or taking away information.

The third and major component of this insurance is computer attack. International media frequently reports that cyber attacks are carried out against a bank, international financial institution; airports and companies suffer millions of losses. This again demonstrates the need for the development of cyber insurance in Georgia. In our country "Aldagi" and "Unisoni" are insurance companies which offer cyber insurance as a new insurance product to modern companies. This insurance product is designed for all the companies processing a large amount of electronic information: banks, airports, clinics and hospitals, state organizations - public and civil registries. The aforementioned policy covers the damages to the first party - the company (recovery of the information, replacement or repair of the servers), as well as damages caused by the suspension of business. For instance, if a bank has stopped working as a result of a cyber-attack, the damage will be covered and the potential profit will be reimbursed. Aldagi cyber insurance also covers the responsibility before the third parties. For instance, if money was withdrawn from the account of the third party, or the personal information of the third party has been leaked, causing it to suffer moral damage, the policy will cover all the losses. Moreover, redemption funds are covered.

Thus, proceeding from the Georgian reality, the innovative product "cyber insurance" offered by insurance companies has been created in cooperation with A+ class European reinsurance companies and covers:

- Loss or spread of personal or confidential information;
- Production of image-damaging or criminal correspondence through the company's communication channels;
- Breakdown of the usual business cycle or an impediment to it;
- Stealing, damaging and erasing databases;
- Damaging the image of the company;
- Cyber blackmail and extortion.

However, the contract on cyber insurance, as a separate form of a contract and its regulatory norms are not envisaged by the Civil Code of Georgia. The terms of the cyber insurance contract are determined in the cyber insurance policy offered by the insurer company to the insurance company. The same contract defines separate details of its legal regulation. The main thing is to determine the precise list of insurance risks the occurrence of which will be considered as the occurrence of the insurance case. The exact amount of the insurance sum, insurance premium and the issue of the sum payable by the insurer company need to be determined.

V. Conclusion

In this paper we have provided the most up-to-date comprehensive survey of available literature on cyber insurance. We have found, that despite a slow start and many problematic issues, the cyber insurance market grows. This growth much depends on the regulatory initiatives applied more widely in the world (e.g., the California bill), but this is not the only cause for the market to flourish. Cyber insurance by itself provides a unique opportunity to cover risks, as well as to contribute to societal welfare. In this work we have considered the main topics tackled in the cyber insurance literature. Moreover, we aligned many scientific contributions with a unique systematising view. Although, the view in no way can be seen as the only possible, fully descriptive and one size fitting all, it allows fast and easy comparison of various studies in the field. The results of the comparison show that although cyber insurance is a desirable option for agents it has many open issues yet to be resolved by scientists and practitioners. Novel approaches and treatments are required to ensure the positive effect of cyber insurance on society as well as new standards and practices required for the maturation of the market. Our study also has provided analysis of different technological systems, which could be or are of interest for cyber insurers. We have found that different technological systems impose different challenges on cyber insurance, and, at the same time, provide different opportunities. Thus, more research is needed to address the needs of cyber insurance in specific contexts. Thus, the cyber threat is not only a technical threat. It is oriented to social media and social networks, and is characterized by complex nature, which once again emphasizes the importance of cyber insurance as an insurance product and the need to actively introduce it on the insurance market. Cyber insurance is the only guaranteed mechanism for protection against negative consequences of cybercrime. However, the need for raising public awareness in this respect is also undoubted and inevitable.

VI. References

Airmic. (2012). Airmic Review of Recent Developments in the Cyber Insurance Market.

Betterley, R. (2012). The Betterley Report: Cyber/Privacy Insurance Markey Survey. The Betterley Reportt.

Bradford, J. (2015) network security & cyber risk management: The fourth annual survey of enterprise-wide cyber risk management practices in Europe, Advisen Ltd.

Baranoff, Etti, Brockett, Patrick Lee, and Kahane, Yehudda (2009). Risk Management for Enterprises and Individuals. Flat World Knowledge Inc., Chapter 8.2.

Böhme, R. Towards Insurable Network Architectures. it - Information Technology, 52, 5 (2010), 290± 293.

Christian C. (2014): Cyber Insurance Basics: an Installment in the Building Blocks Series of Insurance Content Kindle Edition

Ehrlich, I., Becker, G., (1972) Market Insurance, Self-Insurance, and Self-Protection, Journal of Political Economy, 80: 623-648

Godinho M. (2013): Cyber Insurance and Claims Investigation Kindle Edition.

Gladishevskaya A. (2017): Cyber Insurance: a New Instrument for Risk Management. Available at: http://forbes.net.ua/opinions/1426423-kiber-strahovanie-novyj-instrument-risk-menedzhmenta

Johnson, B. Laszka, A Grossklags, J. (2014) The complexity of estimating systematic risk in networks, in: Proceedings of the 27th IEEE Computer Security Foundations Symposium, CSF, 2014

Heal, G., & Kunreuther, H. (2003). Interdependent security. Journal of Risk and Uncertainty, 26(2±3), 231±249

Marsh. (2013). Benchmarking Trends: More Companies Purchasing Cyber Insurance.

Morgan, S. (2015) CyberSecurity Market Reaches; Forbes.

Martinelli, F., Yautsiukhin, A. (2016) Security by insurance for services, in: Proceedings of the 1st International Workshop on Cyber Resilience Economics,

Pal, R. Hui, P. (2017) The impact of secure oss on Internet security: What cyber insurers need to know, Tech. Rep, 2012, arXiv:1202.088, CoRR, available at https://arxiv.org/abs/1202.0885 on 03/01/2017

PartnerRe and Advisen (October 2016) 201 Survey of Cyber Insurance Market Trends.

Schutzer, D. (2015). An Assessment of Cyber Insurance. CTO Corner. Retrieved from http://fsroundtable.org/cto-corner-assessment-cyber-insurance/

Price Waterhouse Coopers. (2015). Insurance 2020 & beyond: Reaping the dividends of cyber resilience. Retrieved from http://www.pwccn.com/home/eng/insurance_2020_sep2015.html

JSC Insurance Company “Aldagi” (2017) available at http://aldagi.ge/ge/

JSC Insurance Company “Unisoni” (2017) available at https://unison.ge/ka

Online Newspaper “Banks and Finances” N 513, October 16, 2017. p.14.

Content Analysis of cyber insurance policies (2017); avaible at https://www.rand.org/content/dam/rand/pubs/working_papers/WR1200/WR1208/RAND_WR1208.pdf

Cyber insurance survey (2017): avaible at https://www.iit.cnr.it/sites/default/files/MARO-17-CSR.pdf

Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as “Compliance Managers” for Businesses available at https://www.law.uci.edu/faculty/full-time/talesh/Talesh-2017-Law%20and%20Social_Inquiry%20Cyber%20

Insurance.pdfBusiness Media Georgia (2019); available at: http://www.bm.ge/ka/article/shss-saqartveloshi-kompiuteruli-danashauli-151-it-gaizarda/28190/

Ministry Interanl Affairs (2018); availble at https://police.ge/files/proeqtebi_reporma%20photos/organizebuli-danashauli/kiberdanashauli-informacia-moqalaqeebistvis.pdf