UDK 338.054.23

The Bonus-Malus System as the policyholders' classification method in cyber-insurance

Ol'ga A. Mirsanova
Post-graduate,
Department of Economics,
Lomonosov Moscow State University,
119991, 1-46 Leninskiye Gory, Moscow, Russian Federation;
e-mail: olga.mirsanova@gmail.com

Abstract

The features of "lemon market" due to information asymmetry characterize cyber-insurance market. Therefore, insurance companies are interested in reducing it. One of the ways to do it is to use a more detailed separation (classification) of policyholders by their estimation simultaneously with a number of the security incidents and the mean failure cost of the incidents during the insurance period. The research consists of four parts. In the first part we reviewed the related publications about cyber-insurance and information asymmetry. The second part shortly describes main features of cyber-insurance market, which are induced by information asymmetry. The third part analyzes the transfer mechanism from one class to another class in the BMS and various parameters of it. Last part includes the "entity-relation" diagram as the data model for the realization of the software for the classification of the policyholders in this way. The article concludes with a summary of the results of this study.

For citation

Mirsanova O.A. (2016) The Bonus-Malus System as the policyholders' classification method in cyber-insurance. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 6, pp. 10-23.

Keywords

Cyber-insurance, information asymmetry, bonus malus system, cyber-risk, classification of policyholders, economic efficiency.

Introduction

According to the current statistics, the quantity of information security incidents grows constantly (see Fig. 1).

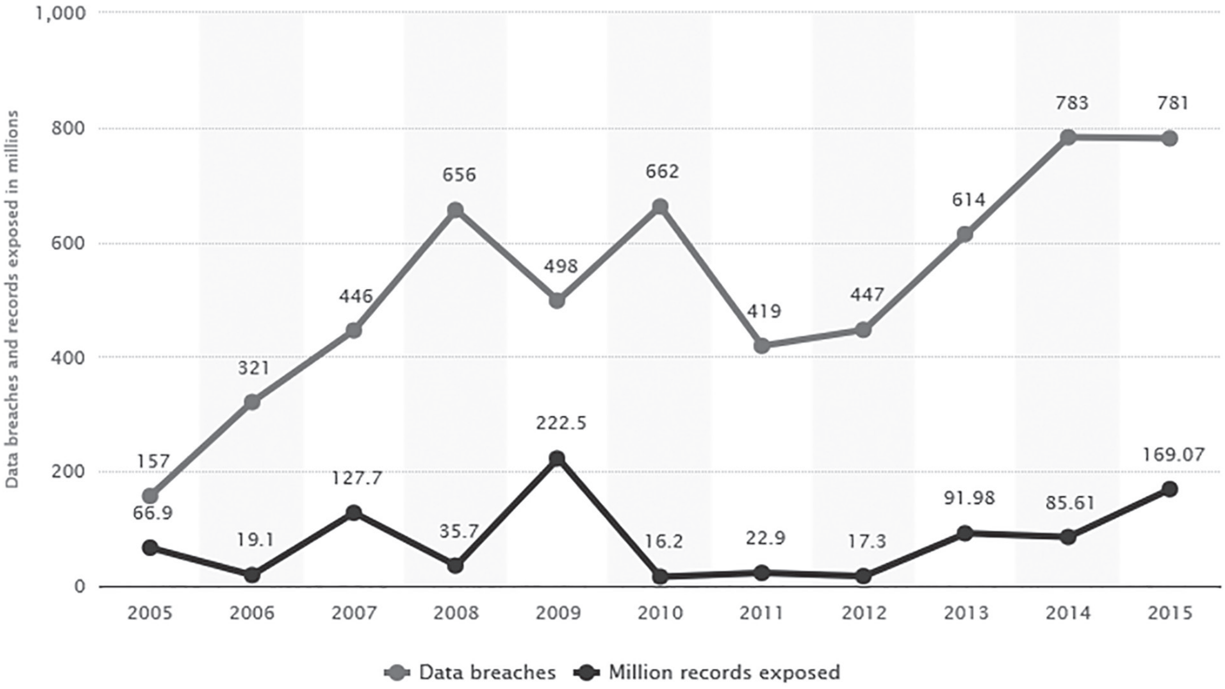

Figure 1. Data breaches and records exposed in millions US dollars in 2005-2015[1]

The annual report of PwC [KPMG…, www] presents that almost 43 million security incidents were detected in 2014 in the world. In other words, there were 100,000 cyber-attacks per day. As for the financial impact of these attacks, large companies (if their revenue is more than $ 1 billion) lost $ 5.9 million, and medium companies lost $1.3 million (revenue is $1 Million – $1 Billion).

Further, the analysts from PwC got response from more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices about information security incidents in the companies in 127 countries in 2015. They concluded that 31.59 percent of respondents had 50 or more information security incidents during 2015 year, 32 percent of respondents had 1-9 information security incidents, 13.46 percent of respondents had no information security incidents, and 7.1 percent of respondents did not know about the number of information security incidents in their companies. The majority of companies (30.53 percent) lost $49,000 or less, and 10.25 percent of companies lost more than $10 million because of information security incidents in 2015. 6.89 percent of respondents did not know about the financial impact of information security incidents in their companies.

As for cyber-insurance, PwC analysts also concluded that 59.36% of companies use cyber-insurance for mitigating their risks. A separate report of Allianz, the German insurer, provided that the "cyber-insurance market could grow to $20 billion by 2025, and there was a general trend toward tougher data protection regimes, backed with the threat of significant fines in the event of a breach" [Insurance 2020 and beyond…, www].

Nowadays many scientific papers are devoted to the idea of cyber-insurance too. These publications describe the following common issues: cyber-insurance market modeling (Böhme,

[1] Sources: Statista.com, 2016.

Schwartz, Shetty, etc.), searching the equation on the cyber-insurance market in the conditions of information asymmetry (Böhme, Schwartz, Shetty, Kataria, etc.), and defining of the attributes of the optimal cyber-insurance contract (H. Herath).

Research motivation

This study was inspired by the ideas of Schwartz, Kamiya, and Lemaire. From one hand, Galina Schwartz approved in her articles (2010) that cyber-insurance market is missing because of adverse selection and moral hazard, even if a deductible used in the contract [Schwartz, Shetty, Walrand, 2010]. The papers of Ogut, Raghunathan, Menon, Shetty, Walrand, Majuca, Yurcik, and Kesan are also devoted to the problem of information asymmetry in cyber-insurance market. From another hand, Jean Lemaire (1985, 1995, 1998) concluded that the bonus-malus approach as the policyholders classification method may help to reduce adverse selection.

Therefore, the main aim of this study is the adaptation of the bonus-malus approach to the cyber-insurance research area in order to find the policyholders classification method based on both a number of incidents and the information security level of a company (a policyholder).

Cyber-risks: main features

The term "cyber-risk" is usually understood in broad and precise meanings. Mukhopadhyay explained it as "the risk involved with malicious electronic events that cause disruption of business and monetary losses" (2005, 2013) and provided the example of its precise meaning. In the broad sense of the word the "cyber-risk" is usually understood as "risk resulting in failure of information systems" [Biener, Eling, Wirfs, 2015]. In other words, cyber-risks refer to the area, which is created as the digital network and used to store, modify, and transfer information.

The insurance regulators provide the following definition of the term "cyber-risk": "operational risks to information and technology asset that have consequences affecting the confidentiality, availability, or integrity of information and information systems" [Biener, Eling, Wirfs, 2015, www].

In addition to this, CobIT5 defines IT risk (it is similar to cyber-risk) as "the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise".

As for cyber-insurance, it is usually understood as it was proposed by R. Böhme and G. Schwartz as "the transfer of financial risk associated with network and computer incident to a third party" [Böhme, Schwartz, 2010, www].

Cyber-risks are caused by the special kinds of information security threats. They are listed below (table 1).

However, cyber-insurance market is very young and has many significant problems. One of them is information asymmetry problem.

Table 1. Cyber-risks caused by the special kinds of information security threats[2]

Threat Level	Objects	List of Threats	Possible methods
Network	Activex-object Interfaces: OLE DB, ADO, ODBC, JDBC Protocols: TCP/IP, IPX/SPX, Named Pipes, Multiprotocol Workstations Servers Rout URL	Listening of the channel	This attack can be in the segment of the network. Thus, a workstation can get packages, which are addressed to other nodes of the network. Therefore, an attacker gets access to all information communications in this segment of the network. Therefore, an attacker should be in the same network segment as an attacked computer.
		Capturing packets in a router	Network route software has access to all packages, which are transferred through the network, so these packages can be captured and over directed.
		Creating a false route	An attacker sends to the network special packages in order to create his own computer as a new router in this network. A false router may be invisible for all or some nodes of the network.
		Replay attack	An attacker sends to the network packages with false address in order to switch over on the own computer connections of the attacked computer/node of the network and collect necessary data from DB Management System.
		Denial-of-Service attack	An attacker sends to the network packages of the special type for networks or computers breakdown.
		Malware implementation	Trojans or smth else for computer data researching, data collection, etc.
Database (DB)	Users Roles Application roles Diagrams Views Tables Rules Functions Data types Triggers Stored procedures Default values	Privacy Threats	SQL injection Inferencing based on functional dependencies Inferencing based on constrained integrity Using UPDATE operator for getting confidential information.
		Accessibility Threats	Using properties of primary and external keys. Records locking for editing. Creating senseless requests for the system. Using malware.
		Integrity Threats	Data modification with the help of SELECT, UPDATE, DELETE operators (SQL)
Database Management System (DMS)	Users Roles Application roles Diagrams Views Tables Rules Functions Data types Triggers Stored procedures Default values	Internal Threats	Attacks by authorized users for increasing users' rights in the system. Occasional mistakes of users Aimed modification of stored data Applications implementations mistakes Hardware implementation mistakes
		External Threats	Hardware failures Viruses and other malware Changes of system configuration Data modification in the channels for information transfer (because of information security incidents)

[2] Source: [Gerasimenko, 1994; Utebov, 2008].

Table 1 continued

Threat Level	Objects	List of Threats	Possible methods
Operational System (OS)	Hardware Software DB files Transaction log files Backup files Transact-SQL, PL-SQL, etc. Services: MSSQL Server, etc.	Key information theft	Password espial Getting a password from the command file Saving the password on the piece of paper near the computer. Password theft by special software
		Password attack	Non-optimized search Optimized search of symbols and bigrams Optimized password search based on the set of probable passwords Optimized password search based on user data Optimized password search based on data of the OS authentication system
		Hard disks scanning	Cascade scanning of hard disk files.
		Shared local network resources scanning	
		Unauthorized access	Getting additional access Starting the software as the user, who has necessary responsibilities. Starting malware as the system software (driver, service, etc.) Data or code modification DLL masquerade
		Denial-of-Service (DoS) attack	Resource locking Hard going or certainly inexecutable request cycling Using mistakes in software

This problem was discussed in several research papers.

1. Schwartz, Shetty, Walrand [Schwartz, Shetty, Walrand, www] focused on adverse selection in cyber-insurance market. They assumed that the probability of an attack depends on the user security level and the network security. They also assumed two user types (malicious and risk averse), where each user has a negligible effect on the network security, malicious users have no damage and normal users have damage D, *D € (0,W)*, where W is the initial wealth of a user if an attack occurs. They argue with Biener [Biener, Eling, Wirfs, 2015, www] and conclude that there is no equilibrium with contracts both with and without deductibles.

2. Shetty, Schwartz, Felegyhazi, Walrand [Shetty, Schwartz, Felegyhazi, Walrand, 2010] focused on only moral hazard problem in cyber-insurance. The authors assumed that all users are identical with identical wealth and identical damage in the case of an attack, the probability of a cyber-attack on a user depends on both user security level and the network security level. Thus, they assumed the existence of an externality. They considered two scenarios. First, if an insurer can contract the network security only (without the user security), a user will not invest in the user security (moral hazard problem exists), so no insurance will be offered in equilibrium (or only minor fractions of damage will be covered). Secondly, if an insurer can contract both the network security and the user security, there will be no

moral hazard problem, however, cyber-insurance will be an instrument of risk redistribution rather than a tool of risk reducing (see [Shetty, Schwartz, Felegyhazi, Walrand, 2010]).

3. C. Biener with his co-authors [Biener, Eling M., Wirfs, 2015, www] specified deductibles and regular risk assessment as moral hazard control methods, and screening and certification as adverse selection control methods.

Using of the bonus-malus system as information asymmetry reducing method

The bonus-malus approach is the rating system, which allows policyholders "to earn bonuses by not filling claims, and a malus is incurred when 08 many claims have been filled" [Kaas et al., 2008]. As some practitioners and theorists state, it helps to reduce information asymmetry in such kind of non-life insurance as automobile insurance. In general, previous researchers studied the bonus-malus systems enough.

The bonus-malus systems (BMSs) were introduced in Europe in the early 1960s, following the works of Bischel (1964), Delaporte (1965), and Buhmann (1964) [Lemaire, 1998]. The bonus-malus system was a key subject of the first ASTIN Colloquium in France in 1959. ASTIN Bulletin and Swiss Actuarial Journal published many researches about BMS. In 1995 J. Lemaire summarized 140 references and complete descriptions of BMS in his book.

Lemaire (the University of Pennsylvania, 1985) called the BMS as "a response to adverse selection about policyholders' behavior" [Lemaire, 1995; Lemaire, 1998]. Therefore, the BMS allows to "partially correct this lack of knowledge about policyholders' driving patterns" [Lemaire, 1995; Lemaire, 1998].

Holtan (2001) analyzed the optimal insurance coverage in the bonus-malus contracts in general terms. He did not include the characteristics of costs and information asymmetry in the expected utility model. He assumed, but not formally proved that "the bonus-malus contracts can only be Pareto optimal" [Holtan, 1999].

Alexander Muermann and Daniela Straka (2011) analyzed the driving behavior of the policyholders in automobile insurance based on the telematics data, which are usually unobservable by insurance companies. They concluded that there were "a positive residual correlation between liability coverage and risk" and a "negative correlation between liability coverage and a number of car rides". However, they noticed, that it is may be misleading to associate these results with information asymmetry [Muermann, Eling, Wirfs, 2011].

Although the bonus-malus approach has been studied in details in automobile insurance, Kamiya stated that practically all researches about it are focused on "the claim frequency effect on the premium" and "the evaluation method featuring adverse selection has not been well defined" [Kamiya, 2006, www]. He explained it in the following way: economists are more interested in searching the market equilibrium and are seldom interested in the searching for the premium rating method, which has influence on the adverse selection. Kamiya studied automobile insurance as the Giffen good and concluded that it helps to define low premiums for good drivers and vice versa. Kamiya finalized that the main reason of the BMS could be defining the penalties for those policyholders who had high level of claim frequency.

Catherine Donnelly and her co-authors [Donnelly, Englund, Nielsen, Tangaard, 2014, www] devoted their research to information asymmetry problem in insurance. They suggested signing the add-on to the insurance contract in order to pay a dividend to the policyholders without the claims during the insurance premium. Their paper proposed to get the additional entrance fee from a policyholder in order to pay him a dividend, if he has no claims in the insurance period.

The bonus-malus approach in cyber-insurance

According to the idea of the bonus-malus systems, we proposed the following possible (not unique and not only correct) method of the policyholders' classification in dependence on their number of claims (as in all BMS) and the impact of the cyber-security incident.

A number of claims are a posteriori characteristic. It means how many incidents were in the insurance period factually.

However, how to measure the impact of the cyber-security incident? This paper uses the mean failure cost (the MFC) as the concrete measure of the cyber-security incident impact in accordance to Frederick Sheldon, Robert Abercrombie, and Ali Mili [Sheldon, Abercrombie, Mili, 2009, www] and the indicator of the economic efficiency of the information security measures.

C. Biener [Biener, Eling M., Wirfs, 2015, www] enumerated several insurability criteria of the cyber-risks.

1) Randomness of loss occurrence (problematic for assessment);

2) Maximum possible loss (not problematic for assessment);

3) Average loss per event (not problematic for assessment);

4) Loss exposure (not problematic for assessment);

5) Cover limits (problematic for assessment);

6) Insurance premium (less problematic for assessment).

Unfortunately, it is hard to assess directly the financial impact of such risks because of the complex structure of the information systems, large quantity of the stakeholders. Therefore, some researchers suggest using the mean failure cost as the value of information security risks.

The cost efficiency evaluation of information protection method

The implementation of the cost efficiency parameter into the bonus-malus system is intended to stimulate the policyholders to increase their information security level and to trace its cost efficiency. It helps to see not only the final number of the information security incidents, but also to evaluate how the policyholders try to mitigate their information security incidents.

Obviously, the basic indicator for this purpose is the efficiency of the information security costs (EC).

$$EC = \frac{TD}{TC}$$

where TC is total costs on the information security facilities (in the insurance period, for example a year), TD is the total damage of the information security incidents in the insurance period.

Total damage (TD) depends on the mean (possible) failure cost per the insurance period.

According to the ideas of Rjaibi, Rabai, Aissa, Levy [Rjaibi, Rabai, Aissa, 2013; [Levy, Ramim, 2010, www] the mean failure cost can be defined in the following way:

1. To define security requirements of the stakeholders (the Stakes Matrix (SM)). The stakeholders should define their requirements, the cost of failing (FC_{ij}) and the probabilities of security requirements delivery (P_j) for each security requirements.

2. To define the accordance between the system components and the security requirements of the stakeholders (the Dependency Matrix (DP)). The system architects and the technical specialists should be responsible for it. In this stage it is necessary to connect the probability of the requirement failing with the probability the system component failing.

3. To define the threats for the system components. The system analysts should be responsible for this. The Impact Matrix (IM) should include the threats for each system component in accordance to the probabilities of these threats (threat probabilities vector (PV)).

4. To define the MFC:

MFC = ST * DP * IM * PV.

Further, we should sum the MFCs of all stakeholders of a policyholder to get the total MFC.

Next, we should multiply the total MFC on the number of the information security incidents to get total damage (TD) of the information security incidents.

Obviously, if the EC is more than 0.5, damage is large and the efficiency of the information security measures is low. It is possible to use it in the BMS in the following way.

To increase the bonus-malus class only if the number of claims is null and the EC is low (less than 0.5).

1. Not to change the number of claims if the number of claims is null, but the EC is high.

2. To decrease the bonus-malus class on 1 if the number of claims is not null and the EC is low.

3. To decrease the bonus-malus class on 2 (or till the minimal class if the current class is 1 or 2) if the number of claims is 1 and the EC is high.

4. To decrease the bonus-malus class on 3 if the EC is low and the number of claims is 2; and to decrease the bonus-malus class on 4 if the EC is high and the number of claims is 2.

5. Additionally, if the number of claims is more than three, the bonus-malus class should be decreased to the minimal class (here – 1).

6. The policyholders transitions matrix is shown, where model *total number of bonus-malus classes* is determined as 6 in accordance to the maturity model by Gartner.

It is possible to modify this decision tree into a set of rules – several inequalities and equalities in dependence on a set of characteristics, which influence the policyholders' classification in the case of simultaneous fulfilment of these conditions.

In other words, for a policyholder it is necessary to define the needful group based on the results of the analysis of the policyholders' characteristics and its interconnections, because it has

Table 2. The bonus-malus classes in accordance to a number of claims and the efficiency of the information security mechanisms[3]

The current class	Class after											
	0 claims		1 claim		2 claims		3 claims		4 claims		5+ claims	
	EC = Low	EC = High	EC = Low	EC = High	EC = Low	EC = High	EC = Low	EC = High	EC = Low	EC = High	EC = Low	EC = High
1	2	1	1	1	1	1	1	1	1	1	1	1
2	3	2	1	1	1	1	1	1	1	1	1	1
3	4	3	2	1	1	1	1	1	1	1	1	1
4	5	4	3	2	1	1	1	1	1	1	1	1
5	6	5	4	3	2	1	1	1	1	1	1	1
6	6	6	5	4	3	2	1	1	1	1	1	1

the influence on the insurance premium. It should help not to create the additional reserves, not to insure malicious clients, and to reduce the insurance cost for the clients without risks. In other words, the dutiful clients should not finance losses of the malicious clients.

Let us describe the possible characteristics of a policyholder for evaluation of the MFC and, finally, define the class of a policyholder.

Table 3. The list of the attributes of a policyholder[4]

№	Attribute	Description	Necessity	Value Type
1	Pholder_id	The identification of the policyholder	Yes	Integer
2	Pholder_name	The name of the policyholder	Yes	String
3	Current_class	The current bonus-malus class	Yes	Integer
4	Number_claims	The number of claims	Yes	Integer
5	Current_ins_period	The current insurance period (year)	Yes	Date
6	Total_ec_value	The EC value	Yes	Numeric
7	ec_high	The EC: high or low.	Yes	Boolean (1 – high, 0 – low)
8	Total_damage	The total damage of the policyholder	No	Numeric

Table 4. The list of the system requirements[5]

№	Attribute	Description	Necessity	Value Type
1	Requirement_group	The information security property - confidentiality, integrity, availability	yes	String
2	Requirement	The requirements for basic information security requirements (confidentiality, integrity, availability).	yes	String
3	Requirement_id	ID of the requirement	yes	Integer

Table 5. The list of the threats[6]

№	Attribute	Description	Necessity	Value Type
1	Threat_id	ID of the threat	yes	Integer
2	Threat_name	The name of the threat	yes	String

[3] Source: developed by the author, based on [Lemaire, 1995; Lemaire, 1998].

[4] Source: described by the author.

[5] Source: described by the author.

[6] Source: described by the author.

Table 6. The list of the bonus-malus classes[7]

№	Attribute	Description	Necessity	Value Type
1	Class_number	The number of the class	Yes	Integer
2	Class_inspremium	The insurance premium for this class	Yes	Numeric

Table 7. The list of the stakeholders[8]

№	Attribute	Description	Necessity	Value Type
1	Stake_id	The identification of the stakeholder	Yes	Integer
2	Stake_name	The name of the stakeholder	Yes	String
3	mfc	The mfc level for the stakeholder	No	Numeric

Table 8. The requirements of the stakeholders[9]

№	Attribute	Description	Necessity	Value Type
1	Requirement_id	The identification of the requirement	Yes	Integer
2	Stake_id	The identification of the stakeholder	Yes	String
3	Component_id	The identification of the system component	Yes	Integer
4	Impact_failing	The financial impact sum in the case of the requirement failing because of this system component	Yes	Numeric
5	Probability_failing	The probability of the requirement failing because of this system component	Yes	Numeric

Table 9. The threats of the system components[10]

№	Attribute	Description	Necessity	Value Type
1	Threat_id	The identification of the threat	Yes	Integer
2	Component_id	The identification of the system component	Yes	Integer
3	Threat_probability	The probability of the threat	Yes	Numeric

These tables are parts of the following possible data model. Such model can be the core part of the special software based on the idea of the policyholders' classification by the efficiency value and the number of claims.

Conclusion

The research adapted the idea of the bonus malus systems to the cyber-insurance sphere. It suggests the idea of the classification of the policyholders as the adverse selection reducing method. It adds the new classification parameter (the mean failure cost) to the standard classification of the policyholders by the number of claims in order to evaluate not only the quantity of incidents, but their impact also.

Risk analysis requires from the specialists to process large volumes of data, sometimes to get these data from the corporate information systems (identity management systems, incident management systems, etc.). So, it is hard to do it manually. The paper suggests the information

[7] Source: described by the author.

[8] Source: described by the author.

[9] Source: described by the author.

[10] Source: described by the author.

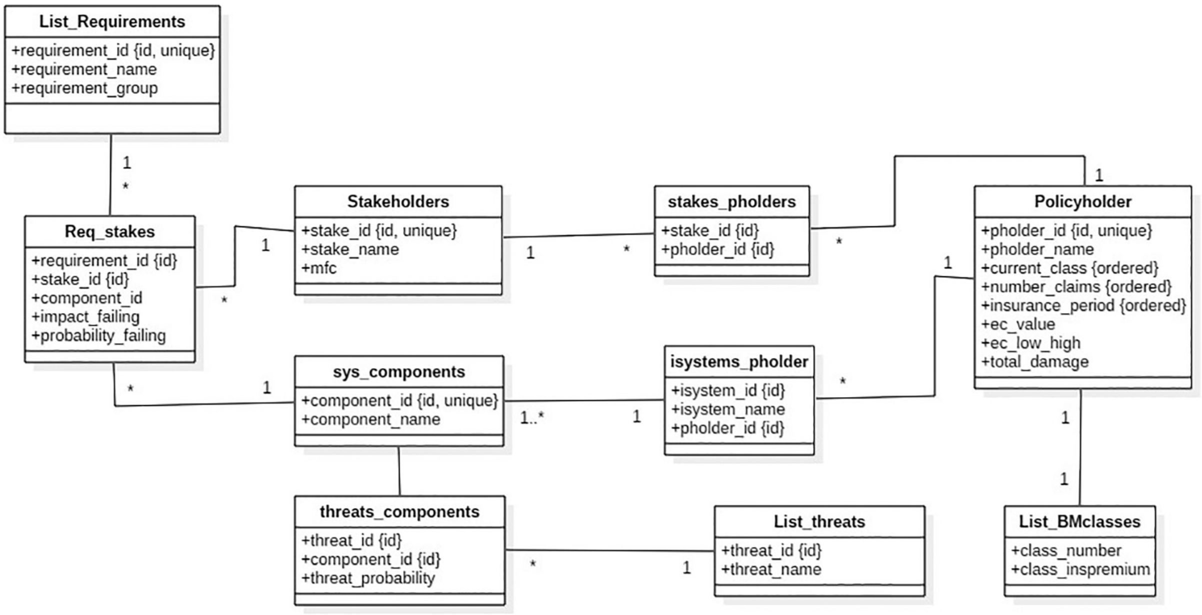

Figure 2. The data model (ERD) of the software for automated policyholders' classification[11]

data model for the software for the classification of the policyholders based on the economic efficiency of the information security measures and the number of claims.

References

1. Biener C., Eling M., Wirfs J.H. (2015) Insurability of cyber risk: an empirical analysis. *Working papers on risk management and insurance*, 151. Available at: http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf [Accessed 15/04/16].
2. Böhme R., Schwartz G. (2010) Modeling cyber-insurance: towards a unifying framework. *WEIS*. Available at: http://econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf [Accessed 12/04/16].
3. Calderon C., Marta E. (2007) A taxonomy of software security requirements. *Avances en Sistemas e Informatica*, 4 (3), pp. 47-56.
4. Cebula J., Young L. (2010) A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*. Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395 [Accessed 12/04/16].
5. Donnelly C., Englund M., Nielsen J.P., Tangaard C. (2014) Asymmetric information, self-selection and pricing of insurance contracts: the simple no-claims case. *Journal of risk and insurance*, 81 (4), pp. 757-780.
6. Firesmith D. (2004) Specifying reusable security requirements. *Journal of object technology*, 3 (1), pp. 61-75.

[11] Source: developed by the author.

7. Gerasimenko V.A. (1994) *Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh* [Data protection in data processing systems]. Moscow: Energoatomizdat Publ.
8. Goldschmidt T., Malek M. (2012) *Ranking of dependability-relevant indicators for availability enhancement of enterprise information systems*. Humboldt-Universität zu Berlin. Available at: http://www2.informatik.hu-berlin.de/sam/preprint/goldschmidt241.pdf [Accessed 11/06/16].
9. Hemantha S., Herath B., Tejaswini, Herath C. (2011) Copula-based actuarial model for pricing cyber-insurance policies. *Insurance markets and companies: analyses and actuarial computations*, 2 (1), pp. 7-20.
10. Holtan J. (1999) Optimal insurance coverage under bonus-malus contracts. *The 30th International ASTIN colloquium*, pp. 43-54.
11. *Insurance 2020 and beyond: reaping the dividends of cyber resilience*. Available at: http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf [Accessed 15/04/16].
12. Jouini M., Aissa A.B., Rabai L., Mili A. (2012) Towards quantitive measures of Information Security: a cloud computing case study. *International Journal of cyber-security and digital forensics (IJCSDF)*, 1 (3), pp. 248-262.
13. Kaas R., Goovaerts M., Dhaene J., Denuit M. (2008) *Modern actuarial risk theory: using R*. Springer Publ.
14. Kamiya S. (2006) *Insurance as a giffen good under a bonus-malus system and its effect on adverse selection*. Available at: http://www.aria.org/meetings/2006papers/Kamiya.pdf [Accessed 15/04/16].
15. *KPMG Cybercrime survey report 2015*. Available at: http://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/Cyber-Crime-Survey-2015-30Nov15.pdf [Accessed 14/04/16].
16. Lemaire J. (1995) *Bonus-malus systems in automobile insurance*. New York: Springer Science + Business Media.
17. Lemaire J. (1998) Bonus-malus systems: the European and the Asian approach to merit-rating. *North American actuarial Journal*, 2 (1), pp. 26-38.
18. Levy Y., Ramim M. (2010) *Students' perceived ethical severity of e-learning security attacks. Proceedings of the chair conference on instructional technologies research 2010*. Available at: http://telem-pub.openu.ac.il/users/chais/2010/after_noon/4_3.pdf [Accessed 14/04/16].
19. Muermann A., Eling M., Wirfs D. (2011) Asymmetric information in automobile insurance: new evidence from telematic data. *NBER insurance workshop*.
20. Rjaibi N., Rabai L., Aissa A.B. (2013) The mean failure cost cybersecurity model toward security measures and associated mechanisms. *International Journal of cyber-security and digital forensics (IJCSDF)*, 2 (2), pp. 23-35.
21. Schwartz G., Shetty N., Walrand J. *Cyber-insurance: missing market driven by user heterogeneity*. Available at: https://people.eecs.berkeley.edu/~schwartz/missm2010.pdf [Accessed 11/04/16].

22. Sheldon F., Abercrombie R., Mili A. (2009) Methodology for evaluating security controls base on key performance indicators and stakeholders issues. *42st Hawaii International Conference on systems science*, pp. 1-10. Available at: http://dblp.uni-trier.de/rec/bib/conf/hicss/SheldonAM09 [Accessed 11/04/16].
23. Shetty N., Schwartz G., Felegyhazi M., Walrand J. (2010) Competitive cyber-insurance and internet security. *Economics of information security and privacy*, pp. 229-247.
24. Tzougas S., Vrontos S., Frangos N. Optimal bonus-malus systems using finite mixture models. Available at: http://repository.essex.ac.uk/11685/1/ASTIN_Essex_Repository.pdf [Accessed 11/04/16].
25. Utebov D.R., Belov S.V. (2008) Ugroza klassifikatsii v sistemakh upravleniya bazami dannykh [Threat classification in database management systems]. *Vestnik AGTU* [Bulletin of Astrakhan State Technical University], 1(42), pp. 87-93.

Система бонус-малус как метод классификации страхователей в кибер-страховании

Мирсанова Ольга Анатольевна

Аспирант,
Экономический факультет,
Московский государственный университет имени М.В. Ломоносова,
119991, Российская Федерация, Москва, Ленинские горы, 1-46;
e-mail: olga.mirsanova@gmail.com

Аннотация

Рынку кибер-страхования вследствие наличия асимметрии информации свойственны черты «рынка лимонов». Поэтому страховые компании заинтересованы в нахождении способа снижения асимметрии информации. Одним из таких методов является более детальная классификация страхователей на основании оценки числа инцидентов информационной безопасности (ИБ) и средней стоимости инцидента ИБ за страховой период. Статья состоит из четырёх разделов. В первой части рассмотрены актуальные публикации в области кибер-страхования и асимметрии информации (в страховании информационных рисков и транспортных средств). Вторая часть вкратце описывает основные характеристики рынка кибер-страхования, которому свойственны черты асимметрии информации. Третья часть содержит анализ механизма перехода от одного класса к другому в рамках системы бонус-малус, а также разные параметры такого перехода. Последняя часть включает диаграмму «сущность-связь», являющуюся моделью данных, на основе которой может быть реализовано программное обеспечение, предназначенное для классификации страхователей с помощью предложенного метода. В заключении статьи изложены результаты исследования.

Для цитирования в научных исследованиях

Мирсанова О.А. The Bonus-Malus System as the policyholders' classification method in cyber-insurance // Экономика: вчера, сегодня, завтра. 2016. № 6. С. 10-23.

Ключевые слова

Кибер-страхование, асимметрия информации, система бонус-малус, кибер-риски, классификация страхователей, экономическая эффективность.