THE INFORMATION CONFIDENTIALITY AND CYBER SECURITY IN MEDICAL INSTITUTIONS

Diana Sabău-Popa [1] **, Ioana Bradea** [2] **, Marcel Boloș** [1] **, Camelia Delcea** [2]

[1] *Department of Finance and Accounting, Faculty of Economics, University of Oradea, Romania*

[2] *Department of Informatics and Cybernetics, Faculty of Economic Cybernetics, Statistics and Informatics,The Academy of Economic Studies, Bucharest, Romania*
dianasabaupopa@yahoo.ro
alexbradea1304@yahoo.com
marcel_bolos@yahoo.com
camellia.delcea@yahoo.com

Abstract: *The information confidentiality and cyber security risk affects the right to confidentiality and privacy of the patient, as regulated in Romania by the Law 46/2002. The manifestation of the cyber security risk event affects the reputation of the healthcare institution and is becoming more and more complex and often due to the: development of network technology, the medical equipment connected to wifi and the electronic databases. The databases containing medical records were implemented due to automation. Thus, transforming data into medical knowledge contribute to a better understanding of the disease. Due to these factors, the measures taken by the hospital management for this type of risk are adapted to the cyber changes. The hospital objectives aim: the implementation of a robust information system, the early threats identifications and the incident reporting. Neglecting this type of risk can generate financial loss, inability to continue providing health care services for a certain period of time, providing an erroneous diagnosis, medical equipment errors etc. Thus, in a digital age the appropriate risk management for the information security and cyber risk represent a necessity. The main concern of hospitals worldwide is to align with international requirements and obtain credentials in terms of data security from the International Organisation for Standardization, which regulates the management of this type of risk. Romania is at the beginning in terms of concerns regarding the management, avoidance and mitigation of information security, the health system being most highly exposed to its manifestation. The present paper examines the concerns of the health system to the confidentiality of information and cyber security risk and its management arrangements. Thus, a set of key risk indicators is implemented and monitored for 2011-2013, using a user interface, a Dashboard, which acts as an early warning system of the manifestation of the risk event in a hospital from western Romania.*

Keywords: information security-cyber security-hospital-Dashboard-ISO.
JEL classification: I10, M10

1. Introduction

Confidentiality of information concerning the patient was a principle respected by physicians from ancient times, as it is stipulated even in the Hippocratic Oath. Respecting the personal aspects of patient's life and ensuring the security of personal information allows the strengthening of physician-patient relation. Due to the development of information technology, the patient related data are recorded in digital databases that are vulnerable to cyber attacks and information leakage generated by an unprotected information system.

Threats related to this type of risk are becoming increasingly powerful, companies and institutions around the world taking action to avoid and mitigate it. The US government has had great concern for this type of risk, the National Institute for Standards and Technology developed a reference framework for this in 2014. The framework has not yet become binding, but companies are encouraged to voluntarily implement it (Callahan, 2014).

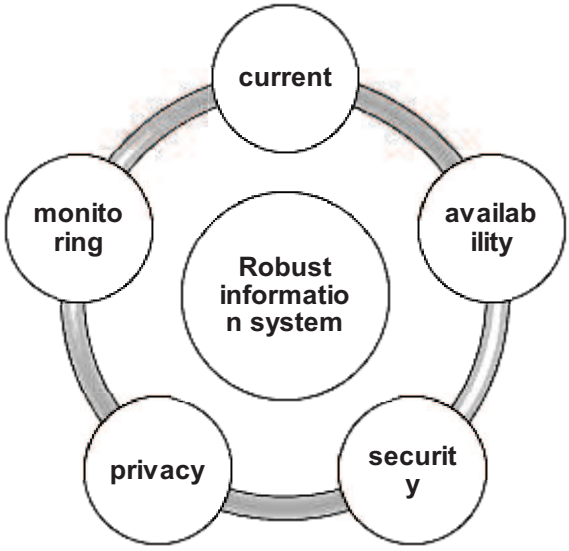
Managing this type of risk can be achieved through: training staff to not provide confidential information without the written consent of the patient, or information and documents belonging to the hospital; regular training for staff; restricting access to people in hospital; encrypting private data regarding personal character, the patient's condition, the medical assistance, the outcome of examinations, diagnosis, treatment and prognosis; releasing the information to the authorized bodies on request and signature; careful recruitment of personnel dealing with the personal information management and cyber security; acquisition of performance software; hiring highly qualified IT-ists; periodic updating of data; periodic checks; rapid communication of errors made through a Dashboard (Bradea, Delcea, Scarlat and Boloș, 2014).

2. Approaches for confidentiality information and cyber security risk management in Romania

Cyberspace provides opportunities to develop a knowledge-based information society, but also risks related to its operation. Due to numerous cyber attacks on institutions all over the globe, risk managers need to be aware of information confidentiality and cyber security risk (Bradea, 2014). Thus, there have been implemented national cyber security strategy in Estonia, USA, UK, Germany and France. Romania is trying to line up with the regulations imposed by ISO: ISO 27001 - "Information technology-Security Techniques-Information Security Management Systems", ISO 27002 – „Information technology-Security techniques -Code of practice for information security controls”, and in the healthcare domain ISO 27799 – „Health informatics-Information security management in health using ISO/IEC 27002”. Also Romania must comply with European directives relating to these issues: 95/46/EC, 2002/58/EC.

Nationally the protection of personal data and their circulation are reglemented by the following laws: 46/2003, 682/2001, 102/2005. Thus, Romania has initiated actions in accord with those of NATO and EU, creating the Romania cyber security strategy and action plan for the implementation of national cyber security. This strategy aimed to: strengthen cooperation between bodies responsible for this area, develop a regulatory framework and a culture of risk management.

Figure 1: Characteristics of a robust information system



Source: Adapted from http://www.iso.org/iso/home.html

The main goal is to create a robust information system that face threats like: cyber attacks, unauthorized access to the system, cyber espionage, blackmail, financial loss, or terrorist activities. The National cyber security system (SNSC) observes the Digital Agenda, which is a Europe 2020 pilot initiative. It has recently been implemented The Romanian Computer Security Incident Response Team (Cert-ro), subordinated to the Ministry for Information Society, Ministry of Internal Affairs, Ministry of Defence and other national institutions. It represents the centre for cyber security incident response; ensures public policies to prevent cyber risk and analyzes the procedural and technical malfunctions in the cyber infrastructure.

But even if at the state level there are concerns related to the management of this risk by facilitating the transition to the information society and strengthening the cyber infrastructure, the healthcare system is particularly exposed to this risk.

Loss of patients personal data is more difficult to detect than in the financial cyber attacks. Exposure to this risk increased this year with the introduction of health cards. Even if they streamline access to patient history, a neglect of security of data stored on these cards can be extremely dangerous. It was observed that in the heathcare system, most cases of data leaks are caused by hospital employees. Vulnerabilities arising from the lack of an integrated security and lack of culture in this area (Delcea, Bradea, Paun, Friptu, 2015).

3. Case Study: Creating an early warning system framework for information security risk in a Romanian hospital

In this section we analyze a set of key indicators for the information confidentiality and cyber security risk, for a Clinical Emergency Hospital situated in western Romania, for a period between 2011 and 2013. Studies on these issues in Romanian literature are scarce, mainly due to lack of data, the hospital managers being reluctant to provide data for research in this area. It can be observed that this type of risk is analyzed using three aspects or variables: system control, system vulnerability and system security.

Most indicators are binary variables that records be 0 (NO) either 1 (YES). The red boxes reflect a high degree of risk, yellow boxes indicate a deterioration in the value of the indicator and the green boxes illustrate values located in the accepted range.

For the information confidentiality and cyber security risk, it is important to consider issues relating to: the security of personal data, data on the patient's condition, the outcome of examinations, diagnosis, treatment and prognosis, the migration to cloud, restricting access to the database, network failure management, careful recruitment of staff dealing with the management of personal information and cyber security, software purchasing performing periodic updating and control of data.

Table 1: Key risk indicators for confidentiality information and cyber security risk

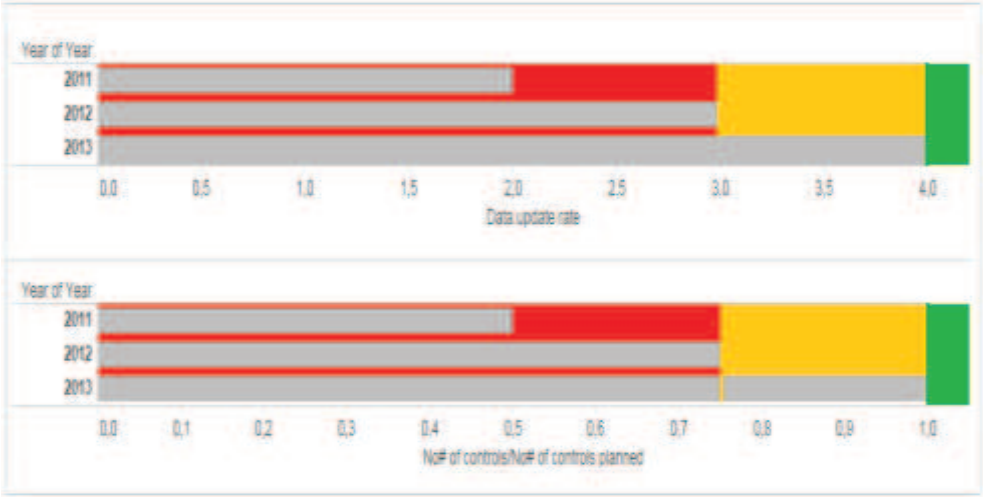
	Variables	Key Risk Indicators	KRI value		
			2011	2012	2013
Confidentiality information and cyber security risk	System Control	Data update rate	3 times /year	4 times /year	4 times /year
		(The number of controls per year/Number of controls planned) * 100	75%	75%	100%
	System vulnerability	Insurance policies for this type of risk	No	No	No
		The number of cyber attacks per year	NO DATA	NO DATA	NO DATA
		The implementation of a management plan	YES	YES	YES
	System security	Unique identification of users	YES	YES	YES
		Automatic users logout password for all equipments	YES	YES	YES

		The ability to remotely wipe data	NO	NO	YES
		Implementation of attacks detection	NO	NO	NO

Source: Own indicators

Medical equipment (such as lasers, glucose monitoring devices, infusion monitoring devices etc.) connected to wifi require permanent monitoring and security because once attacked can provide constant access to data in interacting systems, but can also damage the health of the patient (can even generate death).

Figure 2: Data update rate and system control evolution



Source: Own calculations

Depending on the values established as acceptable for each KRI, are set thresholds that alert the risk manager if there are recorded exceeding. As with traffic lights, exceeding the threshold is indicated by the yellow traffic light. When the risk is situated in the green or yellow area, risk management should take measures to prevent the risk. If the situation is extremely unfavourable and the indicator value is in the red zone, the hospital losses and measures must be taken to mitigate it (Bradea, Delcea, Păun, 2014).

In the figure 2 is presented the evolution of the data update rate and system control. It can be observed that the desired data update rate is four times/year, situation met in 2013. In 2011 the hospital was exposed to the information security risk, being made only two year update data. Regarding the system control, the value of the KRI that reflects the number of controls per year divided to the number of controls planned, also in 2011 the value was in the red zone, and after the taken measures by risk management its value gradually improved until 2013.

3. Conclusions

An ineffective information confidentiality and cyber security risk management in a hospital determine: leakage of sensitive information, medical work breaks due to malfunctions of computer networks, loss of trust and reputation and complaints. These can

cause: errors in diagnosis, medical errors and financial losses, all with disastrous consequences for the healthcare institution.

The analysed hospital is exposed to the information security risk, because many issues that concern this risk management of this type of risk were not implemented. It requires awareness of the negative effects of the manifestation of this risk and an organizational culture that supports continuous improvement in the information system.

4. Acknowledgements

This paper was cofinanced from the European Social Fund through Sectoral Operational Programme Human Resources Development 2007-2013, project number POSDRU/159/1.5/S/134197 „Performance and excellence in doctoral and postdoctoral research in Romanian economics science domain" Also, this work was co-financed from the European Social Fund, through the Sectorial Operational Programmee Human Resources Development 2007-2013, project number POSDRU/159/1.5/S/138907 "Excellence in scientific interdisciplinary research, doctoral and postdoctoral, in the economic, social and medical fields -EXCELIS", coordinator The Bucharest University of Economic Studies.

References

Bradea, IA., Delcea, C., Scarlat, E. and Boloș, M. (2014) "KRIs in Hospitals - Network, Correlations and Influences", *Economic Computation and Economic Cybernetics Studies and Research*, 1/2014, vol. 48, pp. 81-94, ISSN: 0424-267X.

Bradea, I.A. (2014) "Risks in Hospitals. Assessment and Management", *The Romanian Economic Journal*, issue 54, year XVII, pp. 25-37, ISSN: 2286-2056.

Bradea, I.A., Delcea, C., Păun, R.M. (2014) "Managing and Controlling the KRIs in Hospitals", Proceedings of 24rd IBIMA Conference: Crafting Global Competitive Economies: 2020 Vision Strategic Planning & Smart Implementation, Milano, Italia, ISBN: 978-0-9860419-3-8, pp. 1824-1830.

Callahan, M.E. (2014) "Cybersecurity and Hospitals: What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response", *American Hospital Association*, USA.

Delcea, C., Bradea, I., Paun, R., Friptu, A. (2015) "A Healthcare Companies' Performance View through OSN", *Studies in Computational Intelligence: New Trends in Intelligent Information and Database Systems*, Springer, vol. 598, ISBN 978-3-319-16210-2, ISSN: 1860-949X, pp. 333-342.

International Organisation for Standardization, ISO, (2015), http://www.iso.org/iso/home.html - accessed in April 2015

Romanian National Computer Security Incident Response Team, Cert-ro, (2015), http://www.cert-ro.eu/ - accessed in April 2015

CONTEMPORARY IMPLICATIONS OF MORAL HAZARD AND ADVERSE SELECTION FOR INSURANCE FIRMS

Carmen Sandu (Toderaşcu)
"Alexandru Ioan Cuza" University of Iași, Department of Finance, Money and Public Administration, Iași, Romania
carmentoderascu@gmail.com

Abstract: *The present paper approaches the effects of moral hazard and adverse selection for insurance firms in a context where insurances are the foundation of modern life. In this respect, the paper analyses defining elements regarding the contemporary risk, assesses moral hazard, morale hazard, anti-selection and adverse selection on insurance market, and identifies main contemporary implications of moral hazards and adverse selection for insurance policies. The main objective is reached by using inductive and deductive techniques. The main conclusions of these paper refer to the most important solutions for moral hazard and adverse selection.*

Keywords: risk, moral hazard, insurance, adverse selection, franchise, bonus- malus.

JEL classification: G22.

1. Introduction

The insurance industry provides coverage for risks economic, climatic, technological, political and demographic, allowing people to conduct their daily lives and businesses to operate, innovate and grow. The word risk is often used in connection with insurance, finance and banking. Insurance risk is a specific element being subject to any insurance contract. There are many situations in which the insured may influence the likelihood of risks exacerbating environmental objective risk taken into account in determining the scale of insurance premiums, a situation arises the notion of moral hazard. Moral hazard arises because the insured assumes full responsibility for his actions and consequences and therefore tends to behave less cautious than usual, leaving the insurer to assume responsibilities for the consequences of his actions. A standard problem of applied contracts theory is to empirically distinguish between adverse selection and moral hazard.
The present paper approaches risks imminence in the contemporaneity by referring to moral hazard and adverse selection. In this respect, the paper comprises sections related to the main topic such as: an brief analysis regarding the concept of 'risk', a short description of the current economic and financial context in contrast to the main risks of insurance market, an approach of moral hazard and morale hazard, anti-selection and adverse selection respectively the main measures to reduce moral hazard and avoid adverse selection. Our main conclusions refer to an informational deficiency which amplifies the effects of the contemporary risks that are dynamic and complex, affected by moral hazard and anti-selection. All the economic and financial mutations are placed in a political and social context more difficult than in the years before the international.

2. Defining elements regarding the contemporary risk

The concept of *risk* as it is known currently is a reflection of a continuing research made in the insurance market area. The contemporary understanding refers to a loss which may occur in certain assessable circumstances. Its etymological roots are in the thirteenth century, but the current form used in the international financial markets is used since 1741. In the last decades the concept of risk has been developed to the current understanding

without direct connections with similar meanings given by words such as danger or luck. Its development was supported with proper mathematical instruments which associate risks with probability analyses for those circumstances which may lead to significant disequilibria.
Defining the "risk" which may look simple in a linguistic perspectives is not a simple task because there are multiple views regarding its meaning. However, there are some common elements such as the exposure to dangers with implications which differ depending on circumstances. A risk is triggered by both known and unpredictable determinants through specific transmission channels. Their nature may be mechanical, chemical or biological. Specifically, these determinants are in fact fires, meteorological events such as tornadoes, unexpected medical problems or criminal acts. The negative effects of risk manifestation are amplified by hazard.
Nowadays, insurance companies use complex methods in order to assess risks if they have an irregular frequency. In this case, assessing risk is more complicated due to economic, financial and social mutations. Their dynamics cannot be assessed through probabilities and establishing a premium is difficult because the references are missing. The risk is too large and it cannot be assessed such as in the case of static risks which have a certain frequency that make them assessable through mathematical techniques. In this respect, insurance firms may associate a manifestation probability for static risks. Therefore, in the case of dynamic risks, insurance firms must establish a higher value for their premium rates because the probability cannot be assessed and the risk is much higher than in the case of static risks.
The international financial crisis and the current conflicts developed in the Eastern Europe emphasises general risks which are impersonal from the perspective of their causes and effects. In this respect, unemployment, armed conflicts, inflation, earthquakes and floods are important events that are primordial in the strategy adopted by the contemporary insurance firms. These phenomena influence the main economic, social, financial and political characterises inside a country. In addition, there are determined certain evolutions of particular risks generated by the actions taken by individuals (Vaughan, 2014). Some specific events have gained an international importance because most of them are assessed in a larger macroeconomic and financial context.
Nowadays, insurance firms aim to obtain a higher profitability rate than in the previous financial year. In this respect, they don't insure speculative risks such as gambling. Their strategy involves just those activities which imply losses. Therefore, insured risks may be personal, related to property issues, liability risks or resulted from the violation of certain contractual agreements.
During contemporaneity, insurance firms, must manage frauds caused by persons who amplify risk intentionally in the context of informational asymmetry. In addition, insurance firms and supervisors of insurance market don't have the necessary instruments to realise a complete assessment of risks. Given this informational asymmetry, insurance firms refuse to insure certain risks or they prefer applying higher premiums to cover their potential losses.

3. Moral hazard, morale hazard, anti-selection and adverse selection in insurance market

Hazard is a central concept in the contemporary insurance because it illustrates the circumstances which determine risk manifestation. Therefore, a hazard is assessed by insurance firms by considering their typology. In the case of physic hazards, insurance firms establish their premiums by including the assessment made by professionals of the entire physical characteristics. In this respect, a premium is determined by their localisation and the occupancy rate of the building. These technical details are important because physical hazards influence risks manifestation. Nowadays, insurance firms focus on those cases of moral hazards in order to identify if individuals amplify a loss in order to collect the

money accordingly to the contractual clauses. In this respect, assessing moral hazard is a necessary component subscribed to the general strategy of the insurance firm in order to avoid frauds (Saunders and Cornett, 2007).
Insurance market confronts many risks and challenges. A special case which implies profound negative implications for insurance firms is that situation when an individual doesn't manifest attention or he doesn't take all the necessary measures to avoid risk manifestation. This situation describes the concept of morale hazard and it derives from the behavioural patterns of individuals who are insured and became careless because they know that a certain amount of money is assured in any circumstances.
Information deficiencies affect the insurance process and create manifestation conditions for anti-selection and adverse selection. In the first case, anti-selection is a risk assumed by the insurance company in the context of reduced capacity or due to the impossibility to observe all the characteristics of the good insured or the health state of an individual. In these circumstances, the individual insured may hide certain deficiencies in order to obtain money from the insurance firm. Given these circumstances, adverse selection refers to that probability for the insurance company to sign contract with individuals who hide deficiencies of their goods or health status.

4. Main contemporary implications of moral hazard and adverse selection for insurance policies

One of the most important challenges of the modern insurance firm is to manage moral risk. In these circumstances, insurance firms must find an equilibrium point between risks insured and total value of premiums. In addition, it must include in their calculation the possibility for an individual to be careless which amplifies the risk. Their implication is limited to those cases where the potential loss is quantifiable.
In the case of adverse selection, implications may be significant due to the fact that insurance firms cannot have complete information such as in the case of health status. Given these special circumstances, contemporary insurance companies confront with significant difficulties when they establish proper premiums for those individuals who intend insuring a complex risk which have unquantifiable effects. In addition, such risk implies higher premiums which are considered unacceptable by clients because they cannot support them financially. For the insurance firm, the financial effort is higher because a part of their resources are allocated to identify and analyse those cases where moral hazard may occur.

5. Finding proper solutions for moral hazard and adverse selection

The main solutions proposed in the current paper refer mainly to a responsibility transfer from the insurance firm to individuals. In this respect, a franchise system may represent the most proper solution which may be used by the insurance firm in order to establish a percent or a fix sum paid by insured when the risk occurs. In addition, the experience of the insurance firm and of its collaborators is essential in order to identify those cases when moral hazard has a frequency higher than the sector average.
An alternative solution to a franchised system consists in applying limitations by using contractual clauses which would limit the amount of money given to those insured individuals when risks occur.
Applying the aforementioned measures is more efficient if comprehensive analyses are made before signing a contract in order to assess market flexibility. In this respect, actuarial calculations are useful instruments to create adequate insurance products in order to stimulate the market such as co-insurance or the deductions applied to premiums calculations for those individuals who have a positive history (the "bonus-malus" system). In addition, such analyses made on the historical evolution, but also on the current state of an individual would support a clear delimitation between diferent risk categories and helps placing the insured individuals in diferent risk classes ("underwriting").

Nowadays, the measures adopted by the participants involved within insurance market manage to segregate risks and create premises for a better offer of insurance products to be adapted for the characteristics and the needs of each individual.

6. Conclusions

The current economic and financial framework has underlined the capacity of the contemporary insurance firms to manage difficult cases such as moral hazard and adverse selection. In this respect, experience of these firms and complexity of assessment method related to risks are essential.

The underwriting represents a primordial solution because it derives from mathematical calculations. In this manner, an adequate support is given to the insurance firms who don't know the exact state of an individual. Therefore, a smoker has a mortality rate higher than average and he must pay a supplementary amount for the premium than a non-smoker.

For insurance firms, is important to have a sufficient portfolio for each insurance category in order to ensure an informational framework sufficient to elaborate statistical analyses. Premium rate must be calculated in order to have a margin which would ensure a reserve for those periods when costs of damage are much higher than usually.

7. Acknowledgements

This work was cofinanced from the European Social Fund through Sectoral Operational Programme Human Resources Development 2007-2013, project number POSDRU/159/1.5/S/134197 „Performance and excellence in doctoral and postdoctoral research in Romanian economics science domain".

References

Abring, J., Chiappori, P.A. and Pinquet, J. (2013) "Moral hazard and dynamic insurance data", *Journal of the European Economic Association 1,* pp 767-820. Banks, E. (2004) *Alternative risk transfer - Integrated risk management through insurance, reinsurance and the capital markets,* Wiley Finance. Dorfman, M.S. (2007) *Introduction to risk management and insurance,* 9th edition, Pearson International Edition.

Lungu, N.C. (2006) *Bazele asigurarilor,* Iasi: Sedcom Libris.

O.E.C.D. (2005) "Catastrophic Risks and Insurance", *Proceeding Policy Issues in Insurance,* No. 8, pp. 1-55.

Okura, M. (2013) "The relationship between moral hazard and insurance fraud", *The Journal of Risk Finance,* Vol. 14, No. 2, pp 120-128.

Robinson C. and Zheng, B. (2010) "Moral hazard, insurance claims, and repeated insurance contracts", *Canadian Journal of Economics,* Vol. 43, No. 3, pp 967-993. Saunders, A. and Cornet A. (2007) *Financial Institutions Management - a Risk ManagementApproach,* 6th edition, McGraw-Hill Irwin.

Vaughan, J.E. and Vaughan, T.M. (2014) *Fundamental of Risk and Insurance,* 11nd edition, Wiley.

Willet, A. (1951) *The economic theory of risk and insurance,* Philadelphia: University of Pennsylvania Press, pp 14-19