Review of Economics & Finance
Submitted on 27/09/2013
Article ID: 1923-7529-2014-01-57-13
Carla Barracchini, and M. Elena Addessi

Cyber Risk and Insurance Coverage: An Actuarial Multistate Approach[1]

Carla Barracchini (Correspondence author)
Department of Industrial and Information Engineering and Economics
University of L'Aquila (Italy); Via G. Gronchi, 18 – Campo di Pile 67100 L'Aquila ITALY
Tel: +39-0862434883, E-mail: carla.barracchini@ec.univaq.it
Homepage: http://www.ec.univaq.it/barracchini

M. Elena Addessi
UniNettuno - Corso V. Emanuele II, 39, 00186 Rome, ITALY
E- mail: ml.addessi@uninettunouniversity.net

***A*bstract:** This paper suggests a possible alternative, original and supplementary (that is, it does not replace nor keep out those standard procedures which have become legal obligations) solution to the issue of network security, whatever the connection tool may be. The procedures regulating activities of prevention, analysis and management of any cyber-attack (known as cyber risk as well as, in more serious cases when individual is involved, cyber-crime) are increasingly numerous, both in privately-owned concerns and in public administration as well. Hereinafter, a terminal is referred to as any device that can be connected to the web via the Internet and/or Intranet. Therefore, this paper does not aim at suggesting a technological solution – a specific task for antivirus programmer – but at formulating the actuarial premises for coverage in case of cyber damage, also known as cyber-insurance. On the analogy of the coverage regarding health insurance and following an actuarial multistate approach, three levels of damage will be identified with regard to the functionality of the terminal. Two typologies of computer policies are hypothesized: ADC (Activities of Daily Cyber) and GCU (Good Cyber Use).

JEL Classifications: G22, G23, I23

Keywords: Insurance, Cyber risk, Actuarial multistate models, Chapmann-Kolmogorov's Equations.

1. Introduction

Nowadays the Internet creates a network connection among millions of computers, which back up several essential services and control the infrastructures. Information and Communications Technology (or ICT) affect all social classes. In the Council of Europe Convention on cyber-crime, such term is used in order to indicate criminal offences such as those against confidential data, infringement of copyright and related rights (Australian Institute of Criminology, 2006).

[1] The authors thank the Department of Industrial and Information Engineering and Economics, University of L'Aquila(Italy) for the financial support, which has allowed this research to be carried out.

When we talk of risk of cyber piracy (hackers) we mean the possibility for receiving a virus that limits the operation of the terminal (the malfunctioning of a terminal can be caused by an interruption of connection, a loss of data, a transmission of information to an unauthorized third party, a missed access to applications, a limited use of the memory, a reduction of speed – regardless the risk time, both in economic and programmable terms).

Risks arising from being connected to the network are several and can be plagiarism, damage or loss of confidential information as well as that you become the target of programmes that inhibit the correct usage of the software and/or the hardware. In this paper, a via-webconnected (Internet and/or Intranet) terminal (I-pod, I-pad, netbook, e-book) is the object of the coverage.

Cyber risk management tool gives rise to challenges that are typically not considered in traditional business insurance models. Issues related to pricing, adverse selection, and moral hazard are common to all forms of insurance.

In addition, several technology-related characteristics make the pricing of cyber-insurance challenging. To address this, both practitioners and academics have argued for more robust and innovative cyber-insurance pricing models to stimulate increased growth in the cyber-insurance market (Baer, *et al*.(2007); Betterlly (2007); Geer, *et al*.(2003); Oellrich (2003)). Radcliff (2001) states that e-risk models so far have been qualitative as there is a dearth of historical data on claim frequency and claim amount.

He suggests the need to develop actuarial tables by quantifying the risks. Grzebiela (2002) identifies e-risk in terms of technical risk, personal information loss risk, economic risk and societal risk. Gordon, *et al*.(2003) provides a framework that an organization should follow for choosing a cyber-risk protection policy. Matthias, *et al*.(2002) have classified e-risk in terms of strategic risks, operational and systems risks, legal and regulatory risks and financial risk but have not come up with any quantification of e-risk.

Little work has been done with regard to quantifying the risks in terms of the expected loss. Similarly, no work has been done to model the probability distributions of the claim frequency and the claim severity. Ogut, *et al*.(2005) investigate cyber-insurance explicitly from a moral hazard and adverse selection perspective. They show that the interdependence of IT security risk among different firms impacts a firm's incentive to invest in cyber-insurance products.

Bolot and Lelarge (2008) combine recent ideas from risk theory and network modeling in an economic approach to develop an expected utility insurance model. They investigate the interplay between self-protection and insurance. Their results show that using insurance is beneficial since it increases the security of the Internet.

Using utility theory, a model the expected premium an organisation is required to pay, depending on its risk profile (Mukhopadhyay, *et al*.(2005)). Businesses are seeking coverage for the value of the data loss, lost revenue due to loss of data, lost revenue due to repair downtimes, legal expenses for damage to another party, cost of crisis management, notification, credit monitoring and restoration after a data breach, and regulatory fines and penalties (Betterley, 2010).

According to Böhme (2005), cyber-insurance would be a good tool to act against IT security risks but market seems not yet ready to supply cyber-insurance. Böhme (2005) developed such a theory with five steps:

1. "Liability unsolved - Losses occur in any case: instead of the originator, the aggrieved party could demand coverage;
2. "New risks" lack actuarial data - Early satellite starts get coverage as well;
3. High probability of losses - You can even insure warships in wartime;

4. Difficulty to substantiate claims - perhaps this can be interpreted as a combination of residual juridical risks together with high transaction costs;
5. Cyber-risks are accumulation risks - Market concentration causes correlation of claims".

In the literature, cyber-insurance is often suggested as a tool to manage IT security residual risks but the accuracy of premiums is still an open question (Gordon, *et al*.(2003)).

Böhme and Kataria (2006), and Mukhopadhyay, *et al*.(2006) has recognized the value of copula methodology for modeling dependent risks. In the case of insurance, this implies modeling the non-linear dependencies in the pricing variables and using simulation to determine the premiums.

The first approach in the information security literature to integrate standard elements of insurance risk with the robust copula methodology to determine cyber insurance premiums is as in Hemantha, *et al*.(2011). In this cyber-insurance pricing model, the premiums depend on the number of computers affected, the firm level dollar loss distribution, and the timing of the breach event.

The aim of this work is not to propose a technological solution Wang, *et al*. (2000), Wang & Wang (2003), Zou, *et al*.(2004) – a specific task for antivirus programmer – but to propose an actuarial model for the coverage of the consequential cyber risks arising from the use of the net, starting from multistate models for health insurance (Pitacco (1995), Olivieri & Pitacco (2011), Bacinello, *et al*.(2011)).

Multistate models are commonly used in order to analyze personal insurance such as life or health insurance (Barracchini (2007)). They allow traditional concepts to be generalized and extended to highly complex typologies of contract as well.

Furthermore, they split the history of risk into specific "states" representing various characterizations – from demography to health to finance (Addessi, *et al*.(2009)).

In the present work we have extended the use of multistate models to cyber-insurance.

In personal insurance, a sequence of "states" exemplifying an insured risk is given by: life, temporary or permanent disability and death. In cyber-insurance, a sequence of "states" is given by proper working, the extent of the damage to the hardware and/or the software and mainly offences against confidential data.

The present work aims at filling this important research gap by developing a cyber-insurance pricing model, where the premiums shall be calculated on the basis of transition probabilities among states and over time. The space among states and the set of transitions among them shall also be determined. For the sake of simplicity, uncertainty has been limited to the transition probabilities among states only.

In particular, we suppose that an under-contract risk follows the stochastic development that is typical of Markov processes. The contribution in the literature on the subject has been developed into three steps:

(1) A quantitative approach allowing an evaluation of actuarial variables in the field of cyber-insurance;

(2) An original use of multistate models as commonly used in personal insurance (i.e. life or health insurance);

(3) Two typologies of elementary cyber coverage – ADC (Activities of Daily Cyber) and GCU (Good Cyber Use) – have been hypothesized.

Here Section 1 provides a review of the related cyber-insurance literature. Similar to what we have done for health insurance coverage, Section 2 defines the different states representing three levels of damage that will be identified with regard to the functionality of the terminal. Section 3 introduces the probabilistic foundations for the building of elementary models of cyber risk policies – more in details, the probabilities of being in the various states as well as the transition probabilities among states with a fixed level of damage.

We will also show a continual case, thus examining the transition intensity among states in order to satisfy the well-known differential equations by Kolmogorov (Hoem, (1988), Gardiner, (2012)). The last Section, at the end of this work, opens up a discussion on future research directions as well as on market and actuarial implications.

2. The Cyber Risk

Symantec Internet Security Report (Base minima di sicurezza (2002)) has shown that the 64% of new attacks have concerned vulnerability of recent software; this is why antivirus companies have not had enough time to study the holes of the antivirus itself and hackers have had much time to attack. It is clear that old software are safer than new ones. We have therefore identified in the average age of the software set up on the computer the variable corresponding to the age of an individual which, unlike the latter, can change on both the directions (i.e. by means of the installation of new software).

It is necessary to catalogue the cyber risks in order to identify the components both on the basis of the possible insurance coverage. An insurance policy pertains to a risk that refers both to an economic element (a covered interest) and to a probabilistic element (harmful events and their probabilities).

In order to classify the level of seriousness and, therefore, of riskiness of the viruses, Symantec proposes the following:

a) the degree of spread;

b) the seriousness of the damage;

c) the speed of virus propagation.

It is not interesting to classify the viruses on the basis of their technical characteristics, but on the basis of the damages they can provoke.

Similarly to what we have done for health insurance coverage, three levels of damage can be identified with regard to the functionality of the computer:

Table 1. The possible states of damage in Computer Insurance and in Health Insurance

STATE	**Computer Insurance**	**Health Insurance**	STATE
Nd	no damage	self-sufficiency	Ss
Rd	repairable damage	temporary invalidity	Ti
Prd	partially repairable damage	permanent invalidity	Pt
Nrd	not repairable damage	death	D

Table 1 lists the possible states of damage we are going to quantitatively describe below from (5), …, (9) by means of Bartex index, commonly used for health insurance.

We indicate with $(1,\dots,m)$ the m-vector of computer activities (operating system, email management, operation of the programmes, management of the database), and with $(\omega_1,\dots,\omega_m)$ $(\omega_i \in N)$ the vector of the weights attributed to such activities; we define with

$$\alpha_j = \begin{cases} 0 & no\ damage \\ 1 & partially\ repairable\ damage \\ 2 & not\ repairable\ damage \end{cases} \quad (1)$$

the discreet aleatory variable j=1,2,...,m describing the level of damage of the *j-th* computer activity.

In this paper, we assume that $\omega_1 = \cdots = \omega_m = 1$, and if $\omega_i = s$, it is possible to replace such activity with s activity $(i1,\dots,is)$ of weights $\omega_{i1} = \cdots = \omega_{is} = 1$. Similar to the case of health insurance, the Barthel index (Pitacco, 1995), as previously described through the aleatory variable, measures the general level of damage

$$\alpha = \sum_{j=1}^{m} \alpha_j \quad (2)$$

where $\alpha = 0$ corresponds to the level of no damage, or initial level, while $\alpha = 2m$ to the general level of non-repairable damage.

Since the determinations of the aleatory variable α_j can be supposed with regard to the different levels of partially-repairable damage, the formula (1) is replaced with (3)

$$\alpha_j^{\tau} = \begin{cases} 0 & no\ damage \\ \tau & partially\ repairable\ damage \\ 2 & not\ repairable\ damage \end{cases} \quad (3)$$

where $0 < \tau < 2$ and consequently the formula (2) is generalized as follows:

$$\alpha^{(\tau)} = \sum_{j=1}^{m} \alpha_j^{(\tau)} \quad (4)$$

where $\alpha^{(\tau)} = 0$ *it* corresponds to the non-existent general damage and $\alpha^{(\tau)} = 2m$ to the general level of a non-repairable damage.

The probabilistic model of a computer coverage is schematized in Figure 1 below. Just like the construction of multistate models (Barracchini, 2007), each state of the computer match every level of damage:

$$S = \{nd, rd, prd^{(1)}, prd^{(2)}, \dots, prd^{(n)}, nrd\}.$$

The states of a computer are defined through the following equations (5,…,9):

$$nd = \{\alpha: \alpha = 0\} \quad (5)$$

$$rd = \{\alpha: 0 < \alpha \leq \alpha^{(1)}\} \quad (6)$$

$$prd^{(1)} = \{\alpha: \alpha^{(1)} < \alpha \leq \alpha^{(2)}\} \quad (7)$$

$$prd^{(n)} = \{\alpha: \alpha^{(n)} < \alpha < 2m\} \quad (8)$$

$$nrd = \{\alpha: \alpha = 2m\} \quad (9)$$

where $0 < \alpha^{(1)} < \alpha^{(2)} < \cdots < \alpha^{(n)} < 2m$

If $n = 2$ the model is represented by Figure 1 on the next page.

Figure 1 describes any change in the states of damage by means of arrows. All the states may lead to the *nrd* state – i.e. the point-of-no-return state that stands for "death". In this work Figure 1 has been standardized, at first identifying the space of S states, whose general level of damage was called x, (see formulas (12) and (13)) and then naming the initial (or input) state with x_I and the final (or output) state with x_O – both of them being variables in S (see formula (14) and the next ones).

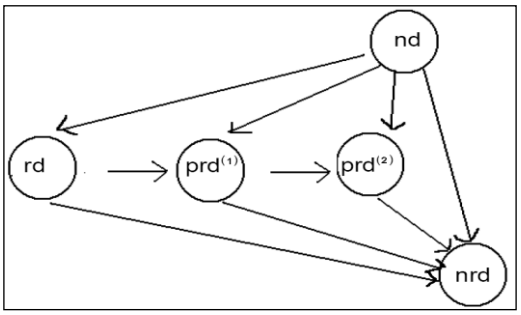

Figure 1. Cyber Multistate Model

3. A Probabilistic Model

In order to present the probabilistic model (as regards life insurance, the probability of death is an increasing function depending on the age of the insured party; as regards health insurance, the probability of not self-sufficiency is an increasing function depending on the age of the insured party, as it can be gathered from the tables of survival), it is necessary to observe that the probability that a software can be damaged by a virus changes according to its time of introduction on the market: if the design and development of software are recent, there will be less possible updates aiming at closing the backdoors.

We indicate with:

- y: the weighted average age of the software contained in a computer (the weights are subjectively assigned to every software component);
- $P(r_x)$: the probability to be r_x days in x state;
- $r_{x(\alpha)}$ the number of the days of permanence in state x with a level of damage α

The unpredictable variable r_x, is the sum of all the dichotomous unpredictable variables $(x \in S)$:

$$\sum_{0<\alpha\leq 2m} \sum_{i=1}^{365} r_{x(\alpha)}^{(i)} = r_x \tag{10}$$

$$\text{with} \quad r_{x(\alpha)}^{(i)} = \begin{cases} 1 & if\ in\ i^{th}\ day\ the\ computer\ is\ in\ x\ status\ on\ \alpha\ level \\ 0 & if\ in\ i^{th}\ day\ the\ computer\ is\ not\ in\ x\ status\ on\ \alpha\ level \end{cases} \tag{11}$$

We are defining the following probabilities through the equations (12,…,16)

$$P_y^x \quad with \quad x \in S \tag{12}$$

the probability that a computer y of average age is in the year of coverage, (from y *to* $y+1$), in x state,

$$_{r_x}P_y^x \quad with \quad x \in S \tag{13}$$

the probability that a computer of y average age is in the year of coverage, (from y *to* $y+1$), in x state for a period of length r_x.

In the probabilities (12) and (13) the initial state is nd; therefore, they result equivalent to the probabilities (12.a) and (13.a) respectively

$$P_y^{nd,x} \quad with \quad x \in S \tag{12.a}$$

$$_{r_x}P_y^{nd,x} \quad with \quad x \in S \tag{13.a}$$

Furthermore, we define with the formula (14) below the probability that a computer of y average age is in the year of coverage, (from y *to* $y+1$), in the state x_I (state of input), and that it can be found, at the end of the year of coverage, in state x_O (state of output).

$$P_y^{x_I,x_O} \ with \quad x_I, x_O \in S \tag{14}$$

The formula (15) shows the probability that a computer of y average age is in the year of coverage (from y *to* $y+1$), in state x_I, and can be found, at the end of the year of coverage, in state x_O, after passing through x state

$$P_y^{x_I,x_O,x} \quad with \quad x, x_I, x_O \in S \tag{15}$$

The formula (16) is the probability that a computer of y average age is in the year of coverage (from y *to* $y+1$), in state x_I, and that it can be found, at the end of the coverage, in state x_O, after passing through x state for a general period r_x:

$$_{r_x}P_y^{x_I,x_O,x} \quad with \quad x, x_I, x_O \in S \tag{16}$$

A list of the features of the probabilistic functions (12,… ,16) is shown below: normality (17), sufficiency (18), Chapmann-Kolmogorov's Equations (19), monotony (20) (Gardiner (2012)).

Normality: probabilistic functions (12,… ,16) ∈ [0,1] (17)

Sufficiency: probabilistic functions (12,… ,16) add up to 1:

$$\sum_{x\in S} P_y^x = 1\,; \quad \sum_{x\in S} {}_{r_x}P_y^x = 1; \quad \sum_{x_O\in S} P_y^{x_I,x_O} = 1 \quad \forall x_I \in S$$

$$\sum_{x_O\in S}\sum_{r_x=0}^{365} {}_{r_x}P_y^{x_I,x_O} = 1 \quad \forall x_I \in S\,; \quad \sum_{x_O\in S}\sum_{x\in S}\sum_{r_x=0}^{365} {}_{r_x}P_y^{x_I,x_O,x} = 1 \quad x_I \in S \tag{18}$$

In the case where we have a discrete variable, we will use the symbol $N = (N_1, N_2, N_3, \dots)$, where the N_i are random variables which take on integral values. We can now write the Chapman-Kolmogorov equation for such a process as

$$P(n_1, t_1 | n_3, t_3) = \sum_{n_2} P(n_1, t_1 | n_2, t_2)\, P(n_2, t_2 | n_3, t_3)$$

This is now a matrix multiplication, with possibly infinite matrices (Gardiner (2012) pag.44).

Informally, this means that the probability of going from state 1 to state 3 can be found among the probabilities of going from state 1 to an intermediate state 2 and then from 2 to 3, by adding up all the possible intermediate states 2.

In this paper, due to the probabilistic functions (12), …, (16), the *Chapmann-Kolmogorov's Equations* (19) become, respectively

$$P_y^{si,x} = \sum_{x\in S}\sum_{x_I\in S} {}_{\tau}P_y^{si,x_I} \cdot {}_{1-\tau}P_{y-\tau}^{x_I,x} \qquad 0 \le \tau \le 1 \tag{19.a}$$

$$ {}_{r_x}P_y^{si,x} = Pr(r_x)\cdot P_y^{si,x} = Pr(r_x)\cdot \sum_{x\in S}\sum_{x_I\in S} {}_{\tau}P_y^{si,x_I}\cdot {}_{1-\tau}P_{y-\tau}^{x_I,x} \quad 0\le\tau\le 1 \qquad (19.b) $$

$$ P_y^{x_I,x_O} = \sum_{x_O\in S}\sum_{x\in S} {}_{\tau}P_y^{x_I,x}\cdot {}_{1-\tau}P_{y-\tau}^{x,x_O} \qquad 0\le\tau\le 1, x_I\in S \qquad (19.c) $$

$$ {}_{r_{x_O}}P_y^{x_I,x_O} = Pr(r_{x_O})\cdot P_y^{x_I,x_O} = Pr(r_{x_O})\cdot \sum_{x_O\in S}\sum_{x\in S} {}_{\tau}P_y^{x_I,x}\cdot {}_{1-\tau}P_{y-\tau}^{x,x_O} $$

$$ 0\le\tau\le 1, x_I\in S \qquad (19.d) $$

$$ {}_{r_x}P_y^{x_I,x_O,x} = Pr(r_x)\cdot P_y^{x_I,x_O,x} = Pr(r_x)\cdot P_y^{x_I,x}\cdot P_y^{x,x_O} = $$

$$ Pr(r_x)\cdot \sum_{x\in S}\sum_{x_1\in S} {}_{\tau_1}P_y^{x_I,x_1}\cdot {}_{\tau-\tau_1}P_{y+\tau-\tau_1}^{x_1,x}\cdot \sum_{x_0\in S}\sum_{x_2\in S} {}_{\tau_2}P_{y+\tau}^{x,x_2}\cdot {}_{1-\tau-\tau_2}P_{y+\tau-\tau_2}^{x_2,x_0} $$

$$ 0\le\tau_1\le\tau_2\le\tau\le 1 \qquad (19.e) $$

With *Normality* and *Sufficiency*, here is the *Monotony:*

$$ P_y^x \ge {}_{r_x}P_y^x \ge {}_{r_x'}P_y^x \quad with \quad r_x' > r_x \qquad (20) $$

The probabilities (12,…,16), which verify the Chapmann-Kolmogorov's equations, describe a trial stochastic discreet Markov (Hoem (1988), Gardiner (2012)pag. 42-51).

Similar to the case of health insurance, we are going to introduce this probabilistic model in the continuous $\{Z(y); y\ge 0\}$ with y as a continuous parameter and $Z(y)\in S$ as a discreet state.

As regards health insurance, the following formula:

$$ {}_tP_y^{x_I,x_O} = Pr\{Z(y+t)=x_0 | Z(y)=x_I\} $$

indicates the probability that a person of age y, in a state x_I x_I , (input state), after t time, and his/her age is therefore $y+t$ $(t>0)$, is in a state x_0 (output state).

In a cyber-contest, through the formulas shown above, we have indicated with y the weighting average age of the software. The age of the software, running on a terminal, is to be referred to as a "biologic age" and not as a "real or calendar age".

After t time, the expiry date of a terminal, $y^* = y+t$, is different from that in health insurance – because the average age of the software changes depending on t: but in the case of the software, if t grows up, the average age of the software itself can also grow up, grow down or remain the same.

The variation of the average age of the software depends on the followings:

The average age y grows up, for example due to the substitution of old software for a new one;

The average age can remain the same because the age of the new software balances the other;

The average age y grows down, due to the placing of newly produced software into the terminal.

If the fluctuation of the average age is negative, a terminal will be younger than it was before the placing of the new software; in this case, we would have a greater probability to infect the terminal, because the antivirus would not be available.

The function of the average age of a terminal and the probability of infection can be described on the basis of a survival table according to the cyber risk.

Such table can be corrected with the age-shifting method that (used in order to correct the longevity risk in life/health insurance), in our case, we can define month-shifting. We have seen the average age change in both directions.

We suppose that a technological asset, such as a computer or another machine connected to the net, can be updated with new software every t months – in other words, its average age can remain the same for t months. This is why the average age changes.

The dynamic probability of damage is given by (21):

$$P_{y:y*}^{x_I,x_O} = Pr\{Z(y^*) = x_O | Z(y) = x_I\} \quad or \qquad (21)$$
$$_tP_y^{x_I,x_O} = Pr\{Z(y+t) = x_O | Z(y) = x_I\}$$

with the probability that a computer of y average age, in x_I state, to y^* average age is in x_O state; and with the (22)

$$\mu_y^{x_I,x_O} = \lim_{y^* \to y} \frac{P_{y:y*}^{x_I,x_O}}{y^* - y} \qquad x_I, x_O \in S, x_I \neq x_O \ \ and \ \ y^* \neq y \qquad (22)$$

the immediate intensity of transition.

With the formula (23), we are defining the total intensity of exit from x_I state

$$\mu_y^{x_I} = \sum_{x_O \in S} \mu_y^{x_I,x_O} \qquad (23)$$

According to actuarial purposes, we are interested in the functions of intensity (22), being they continuous (and limited) or constant at intervals due to their greater easiness to be implemented.

In the case of the homogeneous Markov process, the immediate intensities of transition are considered as constant functions (Hoem (1988)):

$$\mu_y^{x_I,x_O} = \lim_{y^* \to y} \frac{P_{y:y*}^{x_I,x_O}}{y^* - y} = \mu^{x_I,x_O} \qquad (22.a)$$

Following (22), we have (22.b)

$$\mu_y^{x_I} = \sum_{x_I \neq x_O} \lim_{y^* \to y} \frac{P_{y:y*}^{x_I,x_O}}{y^* - y} = \lim_{y^* \to y} \frac{\sum_{x_I \neq x_O} P_{y:y*}^{x_I,x_O}}{y^* - y} = \lim_{y^* \to y} \frac{1 - P_{y:y*}^{x_I,x_O}}{y^* - y} \qquad (22.b)$$

"In probability theory, Kolmogorov equations, including Kolmogorov forward equations and Kolmogorov backward equations, characterize random dynamic processes. Suppose we have a complete statistical description of a stochastic process $x(t)$ and know some transformation (for example, velocity) which defines a new process $y(t)$ related to $x(t)$. Then the Kolmogorov equations are a means for determining features of the stochastic process $y(t)$"(Hoem (1988)).

We now have the tools to write the Kolmogorov's differential equations in the continuous case, fixing the y average age of entry of the computer under insurance coverage.

Kolmogorov's forward differential equations:

Equation (24) is defined as forward, since the average age of entry, y, under an insurance coverage is fixed while the average age of exit y^* changes:

$$\frac{dP_{y:y*}^{x_I,x_O}}{dy^*} = \sum_{x_I \neq x_O} P_{y:y*}^{x_I,x} \cdot \mu_{y^*}^{x,x_O} - P_{y:y*}^{x_I,x_O} \cdot \mu_{y^*}^{x_O} \qquad (24)$$

Kolmogorov's backward differential equations:

Equation (25) is defined as backward, since the two values of the average age of the terminal, y and y^*, operate in opposite ways:

$$\frac{dP_{y:y*}^{x_I,x_O}}{dy} = P_{y:y*}^{x_I,x_O} \cdot \mu_{y^*}^{x_I} - \sum_{x \in S} P_{y:y*}^{x,x_O} \cdot \mu_{y^*}^{x_I,x} \qquad (25)$$

therefore, we have that $y > y*$, $y < y*$ or $y = y*$.

The formula (24) can be obtained on the basis of the equations of Chapmann-Kolmogorov (19.c), properly modified:

$$\boldsymbol{\frac{dP_{y:y^*}^{x_I,x_O}}{dy^*} = \sum_{x_I \neq x_O} P_{y:y^*}^{x_I,x} \cdot \mu_{y^*}^{x,x_O} - P_{y:y^*}^{x_I,x_O} \cdot \mu_{y^*}^{x_O}; \quad \forall x_I, x_O, x \in S, \forall y^*, 0 \leq y \leq y^*}$$

With $\boldsymbol{P_{y:y}^{x_I,x_O} = \delta^{x_I,x_O}}$, as the initial condition, where

$$\boldsymbol{P_{y:(y^*+\Delta y^*)}^{x_I,x_O} = \sum_{x_I \neq x_O} P_{y:y^*}^{x_I,x} \cdot P_{y:(y^*+\Delta y^*)}^{x,x_O} + P_{y:y^*}^{x_I,x_O} \cdot P_{y:(y^*+\Delta y^*)}^{x_O,x_O}}$$

The immediate intensities of transition come from the following relationships:

$$\boldsymbol{\frac{P_{y:(y^*+\Delta y^*)}^{x_I,x_O} - P_{y:y*}^{x_I,x_O}}{\Delta y^*} = \sum_{x_I \neq x_O} P_{y:y^*}^{x_I,x} \cdot \frac{P_{y^*:(y^*+\Delta y^*)}^{x,x_O}}{\Delta y^*} + P_{y:y*}^{x_I,x_O} \cdot \frac{P_{y^*:(y^*+\Delta y^*)}^{x_O,x_O} - 1}{\Delta y^*}}$$

Since $\boldsymbol{1 - P_{y:(y^*+\Delta y^*)}^{x_O,x_O} = \sum_{x_I \neq x_O} P_{y^*:(y^*+\Delta y^*)}^{x_O,x}}$

we have

$$\boldsymbol{\frac{P_{y:(y^*+\Delta y^*)}^{x_I,x_O} - P_{y:y*}^{x_I,x_O}}{\Delta y^*} = \sum_{x_I \neq x_O} P_{y:y^*}^{x_I,x} \cdot \frac{P_{y^*:(y^*+\Delta y^*)}^{x,x_O}}{\Delta y^*} - P_{y:y*}^{x_I,x_O} \cdot \frac{P_{y^*:(y^*+\Delta y^*)}^{x_O,x}}{\Delta y^*}}$$

from which the formula (24) is obtained when $\boldsymbol{\Delta y^* \to 0}$.

However, the study of the conditions of the existence of solutions for the probabilities of transition for which it can be referred to Hoem (1988), lies outside the purposes of the present work.

Demonstration of the Kolmogorov's Backward Differential Equation:

On the basis of analogous reflections,

$$P_{(y-\Delta y):y^*}^{x_I,x_O} = P_{(y-\Delta y):y}^{x_I,x_I} \cdot P_{y:y^*}^{x_I,x_O} + \sum_{x_I \neq x_O} P_{(y-\Delta y):y}^{x_I,x} \cdot P_{y:y^*}^{x,x_O}$$

it follows that the formula (25) comes true:

$$\frac{dP_{y:y^*}^{x_I,x_O}}{dy} = P_{y:y^*}^{x_I,x_O} \cdot \mu_{y^*}^{x_I} - \sum_{x \in S} P_{y:y^*}^{x,x_O} \cdot \mu_{y}^{x_I,x}$$

4. Activities Daily Cyber (ADC) and Good Cyber Use (GCU): Suggesting Two Models of Insurance Coverage

In case of an insurance policy against terminal damages following the use of the net, to every state of damage:

$$nd, rd, prd^{(1)}, prd^{(2)}, \dots, prd^{(n)}, nrd$$

a level of compensation is guaranteed.

If the coverage ADC (Activities Daily Cyber) is adopted, the general compensation for a damage in x state, $x \in S$, is defined by

$$R_x^{ADC} = r_x R_x \tag{26}$$

where r_x is the aleatory number of days necessary to restore the computer to the initial state, nd, from x state of damage. And, R_x is the "daily allowance".

R_x is dependent both on the type of policy and on the operational characteristics of the insured asset; therefore, the general compensation for a damage in state x, $x \in$ S, is defined by a good use of the insured asset.

If the coverage GCU (Good Cyber Use) is adopted, the unique compensation R_α^{GCU}, with regard to the incapability of developing particular cyber activities among the m-listed in the policy, is defined by

$$R_\alpha^{GCU} = \begin{cases} 0 & if \quad 0 \le \alpha < \alpha_{min} \\ R'_\alpha & if \quad \alpha_{min} \le \alpha \le 2m \end{cases} \tag{27}$$

In both these insurance models, the limit of liability and/or the allowance can be used. A policy can contain, separately or jointly, ADC and GCU coverage.

The fair premiums in both cases of coverage are, respectively:

$$\Pi_x^{ADC} = E(R_x^{ADC}) = E(r_x R^{ADC}) = \sum_{0<\alpha\le 2m} \left(\sum_{x(\alpha)\in S} r_{x(\alpha)} R^{ADC} r_{x(\alpha)} P_y^{si,x(\alpha)} \right) \tag{28}$$

$$\Pi_\alpha^{GCU} = E(R_\alpha^{GCU}) = \sum_{x\in S} \left(\sum_{\alpha_{min}\le\alpha\le 2m} R'_\alpha \, P_y^{si,x(\alpha)} \right) \tag{29}$$

On the basis of (29), it is clear that the GCU policy covers all the states of damage, whose level is at least equal to the minimum one previously fixed α_{min}. The analytical study of the expressions of the premium will be the subject of a research next to come: for instance, the initial state, as in the probabilities (28) and (29), is different from nd.

5. Conclusion

The probabilistic model of cyber risks, based on some possible states of damage, is an application of multistate models to the damage insurance.

With the dynamic aspects of premium evaluation, we would like to examine in details the following two:

- if the software changes, the y average age changes;
- if the computer software is modified (set up or erased) during the period of insurance cover, the probability distribution of claim changes.

Without demanding completeness, we strongly believe that building up actuarial models on a multistate level can open a new way to "dynamically" calculate the probabilities of survival/death – above all, if we consider a time variable, in the place of the insured's age, that changes on both the directions (i.e. ageing/rejuvenation). In fact, alongside numerical age, physiological age of risk would be evaluated – thus allowing us to analyze the process itself of ageing and/or rejuvenation.

As regards the premium evaluation, technological indexes or age, even when *ad hoc*, can also be evaluated just like the index-linked contracts.

Already in Barracchini (2007) and then in Addessi, *et al*.(2009) suggested an actuarial model at the basis of the development of a policy that covers risks arising from a network connection, independently from the connection typology and the connection tool.

Nowadays as well as in the years to come, the aim of "having a safe connection" is an increasingly necessary requirement.

References

[1] Addessi, M.E., Annibali, A., Barracchini, C. (2009), "New cyber risk: premises for a coverage about net damages", *International Review of Business Research Papers*, 5(6): pp. 50-62

[2] Australian Institute of Criminology , High Tech Crime Brief, (2006) "Malware- viruses, worms, Trojan horses" ISSN 1832-3413. No.10 of 2006, Available at http://www.aic.gov.au/documents/

[3] Bacinello, A.R., Millossovich, P., Olivieri, A., Pitacco, E. (2011), "Variable Annuities: A Unifying Valuation Approach", *Insurance*: *Mathematics & Economics*, 49(3): 285-297.

[4] Baer, W.S., Parkinson, A. (2007), "Cyber-insurance in IT security management", In: *IEEE Security and Privacy* 5, pp. 50-56.

[5] Barracchini C. (2007), *Modelli multistato nelle assicurazioni di persone*, Roma, Italy: A Book of Aracne Editrice (in Italian).

[6] Base minima di sicurezza Allegato 2 (2002), "*La sicurezza Informatica e delle Tele-comunicazioni (ICT Security)*", Direttiva del Presidente del Consiglio dei Ministri, The Official Journal 22 marzo.

[7] Betterley, R.S. (2007), "The Betterley report. Cyber-risk market survey", [Online] Available at http://betterley.com/ordering.php

[8] Betterley, R.S. (2010), "The Betterley report. Cyber risk and privacy market 2010: one of the hottest new P&C products ever attracts numerous insurers", [Online] Available at http: //betterley.com/ordering.php

[9] Böhme, R. (2005), "Cyberinsurance revisited", *Workshop on the Economics of Information Security* (*WEIS*), Boston: Harvard University, USA.

[10] Böhme, R., Kataria, G. (2006), "Models and measures for correlation in cyber-insurance", *Workshop on the Economics of Information Security* (*WEIS*), Cambridge: Cambridge University, UK.

[11] Bolot, J.C. and Lelarge, M. A. (2008), "New Perspective on Internet Security using Insurance", *IEEE INFOCOM proceedings.*

[12] Gardiner, C.W.(2012), "Stochastic Methods: A Handbook for the Natural and Social Sciences", *Springer Series in Synergetics*, Fourth Edition.

[13] Geer, D., Jr., Hoo, K.S., Jaquith, A. (2003), "Information security: why the future belongs to the quants", *IEEE Security and Privacy*, Vol.1, Issue 4: 24-32.

[14] Gordon L.A., Loeb M.P., Sohail T.(2003), "A framework for using insurance for cyber risk management", *Communications of the ACM*, 46(3): 81-85.

[15] Grzebiela, T. (2002), "Insurability of electronic commerce risks", *System Sciences, HICSS Proceedings of the 35th Annual Hawaii International Conference,* Jan. 7-10, 2002.

[16] Hemantha S.B. Herath, Tejaswini C. Herath (2011), "Copula-based actuarial model for pricing cyber-insurance policies", *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2(1): pp. 7-20.

[17] Hoem, J. M. (1988), "The versatility of the Markov chain as a tool in the mathematics of life insurance", *Transactions of the 23rd International Congress of Actuaries*, Helsinki.

[18] Matthias, B., Drennan, L. and Higgins, A. (2002), "Managing e-risk", *Association of British Insurers*, December issue., Available at www.abi.org.uk/Display/File/364/ERisK_ Ex_Sum.pdf, last accessed 30/6/2005

[19] Mukhopadhyay, A., Saha, D., Chakrabarti, B.B., Mahanti, A., Podder, A. (2005), "Insurance for cyber-risk: a utility model", *Decision*, 32(1): 153-169.

[20] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K. (2006), "E-Risk management with insurance: a framework using copula aided Bayesian belief networks", 39th Hawaii *International Conference on System Sciences*, Jan. 4-7, 2006.

[21] Oellrich, H. (2003), "Cyber-insurance update", *CIP Report* 2, pp. 9-10.

[22] Ogut, H., Menon, N., Raghunathan, S. (2005), "Cyber-insurance and IT security investment: impact of independent risk", *Workshop on the Economics of Information Security* (WEIS). Harvard University, Cambridge, USA.

[23] Olivieri, A., Pitacco, E. (2011), *Introduction to insurance mathematics: Technical and financial features of risk transfers, SPRINGER,* 2011; ISBN:9783642160288

[24] Pitacco E. (1995), *Modelli attuariali per le assicurazioni sulla salute*, A book of *CERAP* no.7, EGEA, Milano, (in Italian).

[25] Radcliff, B. (2001), "Politics, Markets, and Life Satisfaction: The Political Economy of Human Happiness", *The American Political Science Review*, 95(4): 939-952.

[26] Wang, C., J.C. Knight, M. Elder(2000), "On viral Propagation and the Effect of Immunization", Pro. *16th ACM Annual Computer Applications Conference*, New Orleans.

[27] Wang, Y & Wang, C.(2003), "Modeling the effects of timing parameters on virus propagation", *ACM* 1-58113-785-0/03/0010 USA.

[28] Zou C.C., Towsley D., Gong W. (2004), "Email virus propagation modeling and analysis", *Technical Report Univ. Massachusetts*, Amherst.