

# A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments

S. Gritzalis · A. N. Yannacopoulos ·  
C. Lambrinouidakis · P. Hatzopoulos · S. K. Katsikas

Published online: 9 January 2007  
© Springer-Verlag 2006

**Abstract** Day by day the provision of information technology goods and services becomes noticeably expensive. This is mainly due to the high labor cost for the service providers, resulting from the need to cover a vast variety of application domains and at the same time to improve or/and enhance the services offered in accordance to the requirements set by the competition. A business model that could ease the problem is the development or/and provision of the service by an external contractor on behalf of the service provider; known as *Information Technology Outsourcing*. However, outsourcing a service may have the side effect of transferring personal or/and sensitive data from the outsourcing company to the external contractor. Therefore the outsourcing company faces the risk of a contractor who does not adequately protect the data, resulting to their non-deliberate disclosure or modification, or of a contractor that acts maliciously in the sense that she causes a security incident for making profit out of it. Whatever

the case, the outsourcing company is legally responsible for the misuse of personal data or/and the violation of an individual's privacy. In this paper we demonstrate how companies adopting the outsourcing model can protect the personal data and privacy of their customers through an insurance contract. Moreover a probabilistic model for optimising, in terms of the premium and compensation amounts, the insurance contract is presented.

**Keywords** Privacy protection · IT outsourcing · Insurance · Optimal contract

## 1 Introduction

The vast variety of Information Technology (IT) goods and services that are nowadays available, in conjunction with the fact that all these goods and services evolve rapidly with time as part of a highly competitive and demanding market, turns their development and maintenance to an extremely difficult and costly task. The main problem is that an IT service provider needs personnel with specialized expertise in several application domains and, even worse, these domains may be different every other six months. Clearly, someone choosing to adopt this model undertakes a high cost, mainly in terms of labor cost. A new, cost effective, business model is thus necessary for most IT service providers. The fastest growing business model today is that of *IT Outsourcing*. IT outsourcing is the provision of IT goods and services by an external contractor. During recent years, major IT outsourcing companies have exhibited substantial growth in outsourcing revenues, while revenues in other areas actually fell. However, several issues, in

---

S. Gritzalis (✉) · C. Lambrinouidakis · S. K. Katsikas  
Department of Information and Communication Systems  
Engineering, University of the Aegean,  
Karlovassi 83200, Samos, Greece  
e-mail: sgritz@aegean.gr

C. Lambrinouidakis  
e-mail: clam@aegean.gr

S. K. Katsikas  
e-mail: ska@aegean.gr

A. N. Yannacopoulos · P. Hatzopoulos  
Department of Statistics and Actuarial-Financial  
Mathematics, University of the Aegean,  
Karlovassi 83200, Samos, Greece  
e-mail: ayannaco@aegean.gr

P. Hatzopoulos  
e-mail: xatzopoulos@aegean.gr

respect to whether it is legally and technically feasible to outsource on behalf of a client a service to an external contractor, need to be investigated. Most of the times outsourcing a service implies that the external contractor will have access to data that may be personal or/and sensitive, thus putting at stake the privacy of the individuals. It is therefore clear that the outsourcing business model introduces new security and privacy threats. These threats, in case that they occur and cause a security incident, may yield both the company that decided to outsource a service and the company that undertook the provision and maintenance of the service, legally responsible for the misuse of personal data or/and the violation of an individual's privacy; this falls into the provisions of the European Union's Directive 95/46, "*On the protection of individuals with regard to the processing of personal data and on the free movement of such data*". When a company outsources a service to some external contractor it is practically impossible to evaluate the effectiveness of the security measures employed by that contractor and the extent to which these security measures are compliant with the regulations of the legal framework about personal data protection. Therefore, the outsourcing company faces the risk of a contractor that acts maliciously in the sense that she causes a security incident for making profit out of it. Of course, it is always possible that the same security incident happens without the contractor acting maliciously. Whatever the case, both companies are legally responsible for the security incident that may cause disclosure of personal/sensitive data and thus violate the privacy of an individual. Most of the times the consequences of such security incidents are significant financial losses or/and fines. Therefore, companies adopting the outsourcing business model will seek ways to mitigate the aforementioned risks. In this paper we demonstrate how this can be achieved through an insurance company and specifically how to develop a probabilistic model for determining the optimal insurance contract (in terms of premium and compensation amounts). The proposed model is general enough to address any kind of security risks including the privacy related ones. Depending on the choice of the model parameters, we may focus on specific security risks, or on privacy violation. For instance, in the case where security risks are addressed the possible losses can be objectively calculated, while in the case of privacy violation the losses are to a great extent subjective. For example, the fact that personal data may be used without the owner's consent may be extremely important for one person, while of no importance for someone else. The qualitative difference between these two cases calls for different methodology of the loss calculation. For the current paper, we

assume that the loss is given, and focus on the construction of the optimal insurance contract. A detailed study of what kind of loss calculation is called for in different cases of security risks or privacy violation incidents is under current research.

The following section presents the IT outsourcing scenario that will be utilised and explains how an insurance contract fits to it. In Sect. 3 we briefly present related work on the subject. In Sect. 4 we introduce a probabilistic model for the contract, while in Sect. 5 we determine the optimal insurance contract by solving the optimisation problem for the outsourcing company and the contractor. Section 6 presents some extensions of the proposed model and provides pointers to our future research work. A summary of the paper and the conclusions can be found in Sect. 7.

## 2 An IT outsourcing scenario and an insurance contract

Let us consider the following model for IT outsourcing insurance: We have two companies, A and B. Company A is the company that has decided to outsource a service, and company B is the company that has been chosen to undertake the service. Since company A is legally responsible for the project, the actions of company B will affect company A. Company A may observe freely the outcomes of the actions of company B, however, she cannot know in advance what actions company B will make. Since companies A and B are legally bound by their actions they seek for some insurance, offered by an insurance company, henceforth called I, which will compensate A and B in case of security incidents (e.g., disclosure of data, privacy violation).

There are five possible scenario, which in what follows will be called *states of the world*. Companies A and I cannot know in advance which state of the world occurs. As we shall see more clearly later on, company B has control over the occurrence of some states of the world, in the sense that its actions may alter the probability of occurrence of some of the outcomes. The states of the world are as follows:

In state 1, no security incident happens, e.g., no disclosure of data or no deliberate modification, and thus neither A nor B suffers any financial losses.

In state 2 a security incident occurs, but this is not B's fault. The prevention of such an incident may be beyond anybody's power or simply due to negligence of A. An example of this case would be for instance, if A does not describe clearly to B what actions are expected, so that B follows precisely the contract offered to her by A, but this turns out not to be enough. We assume that in this

case, companies A and B will suffer a financial loss of  $L_{A2}, L_{B2}$ , respectively.

In state 3, an accident happens but now due to negligence of B. In this case, eventhough there is good will on behalf of B to fulfill her obligations they prove insufficient for this purpose. We assume that in this case, companies A and B will suffer a financial loss of  $L_{A3}, L_{B3}$ , respectively.

So far, in states 1–3 we assume that company B acts in a *bona fide* way and tries to fulfill as well as possible her obligations towards A. The remaining two states of the world assume that company B acts maliciously, in the sense that she either causes a security incident on her own will to make profit out of it (e.g., violates an individual’s privacy by disclosing data to a third party for her own profit), or in order to reduce the required effort she does not employ all necessary security measures and on account of that causes a security incident. We assume that such a malicious action has a probability,  $d$ , of passing unnoticed, in the sense that the security incident may be characterized as an accident and not attributed to malicious action on behalf of B, and a probability,  $1 - d$ , of being discovered. We call the first case, state 4 and the second case state 5.

In state 4, company A suffers a financial loss  $L_{A4}$  whereas company B, has a financial gain G.

In state 5, company A suffers a financial loss  $L_{A5}$  while company B has to pay a fine F part of which is assumed to go to company A and part of which is assumed to go to the insurer. We will call  $F_A$  and  $F_I$  these parts respectively and assume that  $F = F_A + F_I$ . Therefore, the net position of company A in state 5 would be  $F_A - L_{A5}$  whereas the net position of company B in this state would be  $-F$ . Of course the fine could include legal charges etc but for the sake of simplicity we neglect these for the time being. The states of the world are summarized in Table 1.

We now make the following assumptions concerning the probability of occurrence of these states. Company A, may not know in advance whether B is a fair player or may plan to act maliciously. She assigns a probability  $\nu$ ,  $0 \leq \nu \leq 1$  to the event that B plays fair, and a probability  $1 - \nu$  to the event that B acts maliciously. Let us now assume that given that B plays fair, there is probability  $p_1$  of no security incident at all, proba-

bility  $p_2$  of a security incident, either due to unforeseen circumstances beyond A’s and B’s means or due to negligence of A, and probability  $1 - p_1 - p_2$  of a security incident due to unpremeditated negligence of B. Let us also assume that given that B has acted maliciously, there is probability  $d$  of the fraud passing undiscovered and probability  $(1 - d)$  of it being discovered. Using the calculus of probability A may assign to state 1 the probability  $\nu p_1$ , to state 2 the probability  $\nu p_2$ , to state 3 the probability  $\nu(1 - p_1 - p_2)$ , to state 4 the probability  $(1 - \nu)d$  and to state 5 the probability  $(1 - \nu)(1 - d)$ . For simplicity we will assume that I has exactly the same information on the possible behavior of B as A. On the contrary, company B knows exactly, as is natural, whether she will act maliciously or not, so for her we assume that  $\nu$  may take two values, 0 and 1, depending on whether B acts maliciously, or play fair, respectively.

The insurer I is offering an insurance contract which will alleviate some of the losses of the companies in cases of a security incident (e.g., privacy violation). We assume that both companies A and B enter into an insurance contract with I in the following terms.

Company A will claim compensation of  $c_A$  if a security incident happens by B’s fault but not if it is proved that B’s fault is a result of malicious behavior. That is A will receive  $c_A$  from I, in states of the world 3 and 4. If a security incident happens on account of A’s negligence or otherwise, A will receive compensation  $\gamma_1 c_A$  from I, where  $\gamma_1 \leq 1$ . The case where  $\gamma_1 < 1$  can be considered as some sort of punishment of A by I for her negligence. Therefore, A will receive compensation  $\gamma_1 c_A$  by I in state 2. Finally, if a security incident happens as a result of malicious action of B and this is proved then company A will receive compensation  $\delta_1 c_A$  by I. We now let  $\delta_1$  take arbitrary values. If  $\delta_1 < 1$  then we may consider it as a sort of punishment from I to A for not choosing properly her collaborators. If  $\delta_1 > 1$  we may consider it as some sort of compensation for suffering fraud. Of course we may also have  $\delta_1 = 1$ . So, in state 5, company A receives  $\delta_1 c_A$  by I. Naturally, if nothing happens, i.e., in state 1, A does not receive any compensation from I. To enter this insurance contract, company A will have to pay a premium  $\pi_A$  so as to claim 1 monetary unit in case a

**Table 1** The states of the world and their description

State	1	2	3	4	5
Description	No incident	Incident Not B’s fault	Incident B’s fault negligence	Incident Deliberate by B not discovered	Incident Deliberate by B discovered
Probability	$\nu p_1$	$\nu p_2$	$\nu(1 - p_1 - p_2)$	$(1 - \nu)d$	$(1 - \nu)(1 - d)$

security incident happens without her responsibility, i.e., in states 3 and 4.

Company B will claim compensation of  $c_B$  if a security incident happens by A's fault, that is in state 2. If a security incident happens by her fault but not as a cause of malicious action, that is in states 3 and 4, company B will claim compensation  $\gamma_2 c_B$  for I. We assume  $\gamma_2 \leq 1$ , so that if  $\gamma_2 < 1$  it may be considered as some sort of punishment for B's negligence. If company B acts maliciously and this is discovered, that is in state 5, then she will be asked to pay a fine  $F_I$  to the insurance company. We assume in this paper that  $F_I = f c_B$ , with  $f \geq 0$ . The case where  $f = 0$  corresponds to the case where the whole fine that B will have to pay for discovered fraud will go to company A. Naturally, in state 1, B will get no compensation from I. To enter this insurance contract, company B will have to pay a premium  $\pi_B$  so as to claim 1 monetary unit in case a security incident happens without her responsibility, i.e., in state 2.

The terms of the contract are summarized in Table 2 while in Table 3 we present the net financial position of the three parties in all different states of the world.

### 3 Related work

Important problems that arise in IT outsourcing environments have been studied in depth for many years, especially from the management and economic point of view [6, 10, 16]. Emphasis has been given to the outsourcing issues in the software development process [5, 20, 22]. More specifically Aubert and coworkers [4] identify the main undesirable outcomes that may result from an IT outsourcing deal. Afterwards they use transaction cost and agency theory as a primary theoretical basis, and propose a framework for categorizing risk factors, which have been identified. Finally they discuss the dynamics of risk, by examining how the various risk factors are linked to undesirable outcomes. In a followup paper Aubert and coworkers [3] define the concept of risks and of risk exposure and apply these definitions to the context of IT outsourcing risk. Moreover, they present a framework of IT outsourcing risk exposure and describe three case studies, each of which lead to a different set of lessons learned on how firms actually manage IT outsourcing risks. In the same direction, Wu et al. [23] develop an analytical model of IT outsourcing

**Table 2** Financial input and output for the contract participants in the different states of the world

State	1	2	3	4	5
Company A					
Loss	–	$L_{A2}$	$L_{A3}$	$L_{A4}$	$L_{A5}$
Compensation by I	–	$\gamma_1 c_A$	$c_A$	$c_A$	$\delta_1 c_A$
Compensation by B	–	–	–	–	$F_A$
Premia to I	$\pi_A c_A$	$\pi_A c_A$	$\pi_A c_A$	$\pi_A c_A$	$\pi_A c_A$
Company B					
Loss	–	$L_{B2}$	$L_{B3}$	–	–
Compensation by I	–	$c_B$	$\gamma_2 c_B$	$\gamma_2 c_B$	–
Premia to I	$\pi_B c_B$	$\pi_B c_B$	$\pi_B c_B$	$\pi_B c_B$	$\pi_B c_B$
Gain	–	–	–	$G$	–
Fines	–	–	–	–	$F = F_A + F_I$
Insurer I					
Premia from A	$\pi_A c_A$	$\pi_A c_A$	$\pi_A c_A$	$\pi_A c_A$	$\pi_A c_A$
Compensation to A	–	$\gamma_1 c_A$	$c_A$	$c_A$	$\delta_1 c_A$
Premia from B	$\pi_B c_B$	$\pi_B c_B$	$\pi_B c_B$	$\pi_B c_B$	$\pi_B c_B$
Compensation to B	–	$c_B$	$\gamma_2 c_B$	$\gamma_2 c_B$	–
Compensation from B	–	–	–	–	$F_I$

**Table 3** Net position for the contract participants in the different states of the world

State	1	2	3	4	5
A net	$-\pi_A c_A$	$-\pi_A c_A - L_{A2} + \gamma_1 c_A$	$-\pi_A c_A - L_{A3} + c_A$	$-\pi_A c_A - L_{A4} + c_A$	$-\pi_A c_A - L_{A5} + F_A + \delta_1 c_A$
B net	$-\pi_B c_B$	$-\pi_B c_B - L_{B2} + c_B$	$-\pi_B c_B - L_{B3} + \gamma_2 c_B$	$-\pi_B c_B + G + \gamma_2 c_B$	$-\pi_B c_B - F$
I wrt A	$\pi_A c_A$	$\pi_A c_A - \gamma_1 c_A$	$\pi_A c_A - c_A$	$\pi_A c_A - c_A$	$\pi_A c_A - \delta_1 c_A$
I wrt B	$\pi_B c_B$	$\pi_B c_B - c_B$	$\pi_B c_B - \gamma_2 c_B$	$\pi_B c_B - \gamma_2 c_B$	$\pi_B c_B + F_I$

For company A we may add at all states of the world  $w_A$ , the initial wealth of company A, whereas for company B we may add for all states of the world  $w_B$  the initial wealth of company B

using Principal Agent techniques. They apply this model in one particular segment of the IT outsourcing market, the market for large-scale packaged software implementations such as ERP systems. Basu et al. [7] have developed a model of testable propositions for applying Agency Theory to study the relationship between implementation consultants and client organizations deploying enterprise resource planning (ERP) systems and to evaluate how the relationship affects the implementation success. Keil [15] is using Principal Agent Theory, an economic research area that is common in all sorts of relations in which a customer's profit or payoff depends on the behavior of a contractor. He describes the economic foundation of outsourcing relationships during the software development process and presents applicable suggestions how to diminish or avoid problems that arise when selecting the "best" contractor during a project.

The last 5 years interesting research work has been published in the area of Security and Privacy Economics. Anderson [2] argues that many computer security problems arise because of perverse economic incentives. In this paper well-known economic concepts are introduced in the context of security engineering, such as information asymmetry, moral hazard, switching costs, etc. Odlyzko [19] examines and explains one of the most important cybersecurity issues, the loss of privacy; organizations have the ability to increase their income by charging different prices to different customers (i.e., price discrimination). While price discrimination leads to efficient allocation of resources, many individual consumers are worse off than when firms charge a uniform price. Since firms have the incentive to collect private information, a continued loss of privacy and use of variants of price discrimination are predicted. Acquisti [1] traces the development of the economics of privacy, with particular emphasis on studies applying microeconomic analysis to issues of privacy in the context of computer networks and electronic commerce.

Significant emphasis has been given in the Evaluation of IT Security Investments. Gordon et al. [12] present an economic model that characterizes the optimal monetary investment to protect a given set of information. In this paper it is shown that, for a given potential loss, the optimal amount to spend to protect an information set does not always increase with increases in the information set's vulnerability. Schechter et al. [21] model the expected profits to a thief of exploiting a single vulnerability in a packaged system that has been installed in multiple organizations. The probability that a given organization's system will be attacked depends on the thief's potential benefits, as well as the preventive actions taken by all the user organizations. Cavusoglu

et al. [9] present an analytical model in an attempt to facilitate decisions regarding security investments. This model provides insight into evaluating the interaction among different technologies and deciding on investments in multiple technologies. Bodin et al. [8] describe how a chief information security officer can apply Analytic Hierarchy Process tool, to determine the best way to spend a limited information security budget and to make a case top the organization's chief financial officer for an increase in funds to further enhance the organization's information security. More recently, Gordon and Loeb [14] provide a general guide for managers dealing with the economic and financial aspects of information security.

The published papers dealing with security and privacy insurance issues are very few. According to Gordon et al. [13] the insurance companies, while designing new policies to deal with the cyber risks of information breaches, must address issues related to pricing, adverse selection, and moral hazard. In this paper the authors examine the unique aspects associated with cyber risks and present a framework for employing an insurance contract as a tool for the management of information security risks. This framework is based on the risk management process and includes a four-step cyber risk insurance decision plan. According to Lambrinoudakis et al. [18], in the absence of a scientifically sound methodology for evaluating the cost-effectiveness of the security measures employed, the problem is that the IT officials are unable to quantify the security level of their system and thus to determine the appropriate amount that they should invest for its protection. An alternative option that organizations can explore is to insure their information systems against potential security incidents, aiming to balance the consequences that they will experience, in terms of financial losses, through the compensation that they will get from the insurance company. Even in that case, though, the difficulty for the insurance company is the calculation of the appropriate premium. In [18], our research group presents a probabilistic structure, in the form of a Markov model inspired by work of Haberman and Pitacco in actuarial science [11], used to provide detailed information on the transitions of the system from the fully operational state to other non-fully operational states that may result as the effect of a security incident. This probabilistic structure enables both the estimation of the insurance premium and the valuation of the security investment.

The present paper tries to combine the concept of using an insurance contract for an information system with the concept of using the methodology of principal-agent type theories to design an optimal contract

between two parties. In the proposed model, we include a third party, the insurer, and through the optimal design of the insurance contract we try to ensure that the agent will have no incentive to indulge into fraudulent behavior even though this may be financially attractive. Furthermore, the insurance contract covers both the agent and the principal against unfortunate states of the world which may lead to losses but without any malice involved on the agent's part. To the best of our knowledge, it is the first time the problem of insurance in IT outsourcing environments is introduced and modeled in this manner. Even though our model is fairly simple, it helps capture the essential ingredients of what a well designed IT outsourcing insurance contract should achieve and thus may help as a guideline to the design of actual (real-life) contracts. Furthermore, as the section on possible extensions of the present paper points out it may be extended to include other more complicated features. With no doubt, such features will require computational techniques for the determination of the optimal contract, but this is a perfectly feasible task which is under active consideration by our research group.

#### 4 A model for the contract

We now make a probabilistic model for this contract.

We assume that both A and B are risk averse rational agents which act so as to maximize their respective utility functions  $u_A(w_A)$  and  $u_B(w_B)$ , which are functions of their wealth. We also assume that choice under uncertainty is made by the maximizing utility functions which satisfy the expected utility property. We further assume that the insurance business is a competitive business, so that there are many contract offers which allow the companies A and B to choose the one that suits them best.

Let us consider separately the problem that each of the parties entering the contract will solve.

##### 4.1 Company A

Company A will choose the insurance contract so as to maximize her expected utility. For future reference we define the function

$$\begin{aligned} U_A(v; c_A, \pi_A) &= v\{p_1 u_A(w_A - \pi_A c_A) \\ &\quad + p_2 u_A(w_A - \pi_A c_A - L_{A2} + \gamma_1 c_A) \\ &\quad + (1 - p_1 - p_2) u_A(w_A - \pi_A c_A - L_{A3} + c_A)\} \\ &\quad + (1 - v)\{d u_A(w_A - \pi_A c_A - L_{A4} + c_A) \\ &\quad + (1 - d) u_A(w_A - \pi_A c_A - L_{A5} + F_A + \delta_1 c_A)\} \end{aligned}$$

This corresponds to the expected utility of company A in the different states of the world that may be realized. For instance, if everything goes well, company A will undergo no loss, but will have to pay the premium. In this state of the world, the wealth of company A will be  $w_A - \pi_A c_A$ , and since this state will be realized with probability  $\nu p_1$  this will contribute to the expected utility of company A by the term  $\nu p_1 u_A(w_A - \pi_A c_A)$ . In the state of the world 2, the wealth of company A will be  $w_A - \pi_A c_A - L_{A2} + \gamma_1 c_A$  (we are adding algebraically the loss of the company  $L_{A2}$  in this case, the insurance contract costs  $\pi_A c_A$  and the compensation  $\gamma_1 c_A$ ). Since this state occurs with probability  $\nu p_2$  this will contribute to the total utility function the term  $\nu p_2 u_A(w_A - \pi_A c_A - L_{A2} + \gamma_1 c_A)$ . In a similar way we calculate the contribution of the other states of the world in the expected utility and formulate the total expected utility for company A. Table 3 in conjunction with Table 1 may be used to justify the form of the utility function for company A.

We assume that A will choose  $c_A$  so as to solve the maximization problem

$$\max_{c_A} U_A(v; c_A, \pi_A)$$

##### 4.2 Company B

Company B has the choice over the action of whether to act maliciously or not. For future reference we define the following function

$$\begin{aligned} U_B(v) &= v\{p_1 u_B(w_B - \pi_B c_B) \\ &\quad + p_2 u_B(w_B - \pi_B c_B - L_{B2} + c_B) \\ &\quad + (1 - p_1 - p_2) u_B(w_B - \pi_B c_B - L_{B3} + \gamma_2 c_B)\} \\ &\quad + (1 - v)\{d u_B(w_B - \pi_B c_B + G + \gamma_2 c_B) \\ &\quad + (1 - d) u_B(w_B - \pi_B c_B - F)\} \end{aligned}$$

This is the expected utility function for company B, taking into account the five possible states of the world that may be realized. For instance if state 1 is realized company B will only have to pay its premia to the insurance company, so that its final wealth in this state would be  $w_B - \pi_B c_B$ . State 1 occurs with probability  $\nu p_1$  so the contribution to the total utility from this state would be  $\nu p_1 u_B(w_B - \pi_B c_B)$ . Similarly for the other states. Table 3 in conjunction with Table 1 may be used to justify the form of the utility function for company B. We do not include explicitly a financial gain for company B in the state of the world 5, where B has committed fraud but has been discovered. Instead, in order to reduce the model parameters, we implicitly take this possibility into account through the possible reduction of the term  $F$ ,

which models the fine that this company must pay in the case of discovery of the fraud.

The insurance contract will have to be so that it solves the following problem

$$\begin{aligned} & \max_{c_B, i \in \{0,1\}} U_B(i) \\ & \text{subject to} \\ & U_B(1) \geq U_B(0) \end{aligned}$$

The constraint is the incentive constraint that will induce B to act fairly. As we will see later on, this constraint is always satisfied if the fines and the probability of discovery of malicious behavior are chosen properly. Constraints of this type are commonly used in the theory of incentives (see e.g., [17]).

This problem is written equivalently as

$$\begin{aligned} & \max_{c_B} U_B(1) \\ & \text{subject to} \\ & U_B(1) \geq U_B(0) \end{aligned}$$

### 4.3 Insurer I

Assuming a highly competitive market, the insurer needs to calculate the premium of the contract for A and B in such a way as her expected gain to be equal to zero. The calculated premium is the absolute minimum for the insurer, since below that she will start losing money. There are more than one ways for I to set the premia. We choose to elaborate here on a way that simplifies the calculations and may thus lead to analytic solutions. In a separate section we propose other methods and outline other possible approaches.

We assume that the insurer sets the premia treating its position by entering the contract with A and B separately. That is the insurer wishes to choose the premia in such a way as to set at the same time the expected gain of the transactions with A to 0 (set the premium for A to its minimum value for I not to lose money) and the expected gain of the transactions with B to 0 (similarly, set the premium for B to its minimum value). This way of setting the premia is fair on A, in the sense that I does not transfer to A the risk she faces from a possible fraud of B. At the same time B will have to pay for her possible unreliability by a higher premium rate. We assume, that I estimates the probability of fraudulent behavior of B as  $1 - \nu$ , that is in the same manner as A. Of course this is an assumption made to simplify matters, which may be raised if necessary.

### The premium for A

Acting as above, I sets the premium  $\pi_A$  by solving the equation  $E[G_A] = 0$  where  $G_A$  is the gain from transactions with A. According to our model this equation becomes

$$\begin{aligned} & \nu\{p_1\pi_A c_A + p_2(\pi_A c_A - \gamma_1 c_A) \\ & \quad + (1 - p_1 - p_2)(\pi_A c_A - c_A)\} \\ & \quad + (1 - \nu)\{d(\pi_A c_A - c_A) \\ & \quad + (1 - d)(\pi_A c_A - \delta_1 c_A)\} = 0 \end{aligned}$$

which readily gives

$$\pi_A = \nu\{1 - p_1 - (1 - \gamma_1)p_2\} + (1 - \nu)\{d + \delta_1(1 - d)\}.$$

We observe that the premium per unit coverage is independent of the total coverage asked (i.e., independent of  $c_A$ ) a fact that simplifies the determination of the optimal contract considerably.

*Remark 1* The premium charged by the insurer I, for company A simplifies considerably in the case where  $\gamma_1 = \delta_1 = 1$ . In this case  $\pi_A = 1 - \nu p_1$ . We see that this premium takes its lowest value in the case where  $\nu = 1$ , i.e., there is no probability of fraud on behalf of company B and takes its largest value in the case  $\nu = 0$ , i.e., when there is high probability for fraudulent behavior on behalf of company B.

*Remark 2* One also sees that in the general situation where the compensation reductions  $\gamma_1$  and  $\delta_1$  are allowed, these may be chosen in such a way as to make the premia for A independent of the probability of fraud on behalf of B. This will happen as long as

$$\gamma_1 p_2 - \delta_1(1 - d) = p_1 + p_2 + d - 1.$$

Notice that  $p_1 + p_2 + d - 1$  is not necessarily a negative number.

### The premium for B

We assume that I takes the same route in the determination of the premium for company B, that is she calculates the premium by solving the equation  $E[G_B] = 0$  where  $G_B$  are the net gains by the transactions with company B. This equation takes the form

$$\begin{aligned} & \nu\{p_1\pi_B c_B + p_2(\pi_B c_B - c_B) \\ & \quad + (1 - p_1 - p_2)(\pi_B c_B - \gamma_2 c_B)\} \\ & \quad + (1 - \nu)\{d(\pi_B c_B - \gamma_2 c_B) \\ & \quad + (1 - d)(\pi_B c_B + f c_B)\} = 0, \end{aligned}$$

where we recall that  $F_1 = f_{CB}$  is the fine paid by B to I if fraudulent behavior is discovered. We readily find that

$$\pi_B = v\{p_2 + (1 - p_1 - p_2)\gamma_2\} + (1 - v)\{\gamma_2 d - (1 - d)f\}.$$

We observe that the introduction of the fine  $f$  helps in the reduction of the premium for B. This is reasonable as the fine may be considered as some state dependent premium.

Furthermore, one sees that  $\frac{\partial \pi_B}{\partial d} = (1 - v)(\gamma_2 + f) > 0$  that is the premium for B increases as the probability of committing undiscovered fraud increases. This is also a very reasonable result.

*Remark 3* One easily sees that the fine may be chosen in such a way as to make the premium charged by I to B independent of the probability of fraud. We see that  $\frac{\partial \pi_B}{\partial v} = 0$  as long as  $f^* = \frac{p_1}{1-d} - 1$ . This fine increases as  $d$  takes values close to 1 that is as the probability of committing undiscovered fraud on behalf of company B increases, as is expected.

*Remark 4* In the special case that  $\gamma_1 = \delta_1 = \gamma_2 = 1$  we observe that

$$\pi_A - \pi_B = -(1 - v)\{d - (1 - d)f\}.$$

We thus see that  $\pi_B < \pi_A$  as long as  $f > f^* = \frac{d}{1-d}$  that is the introduction of a fine which is larger than the critical value  $f^*$  will allow the insurer to charge lower premia to B than to A.

### 5 Solution of the model and the optimal contract

We now solve the optimization problem for A and B and determine the optimal insurance contract.

#### 5.1 The contract for A

We start with the optimization problem for A. This is a standard optimization problem and the optimum can be found by solving the first order condition

$$\begin{aligned} 0 = & -v\{p_1\pi_A u'_A(w_A - \pi_A c_A) \\ & + p_2(\gamma_1 - \pi_A)u'_A(w_A - \pi_A c_A + \gamma_1 c_A - L_{A2}) \\ & + (1 - \pi_A)(1 - p_1 - p_2)u'_A(w_A - \pi_A c_A + c_A - L_{A3})\} \\ & + (1 - v)\{d(1 - \pi_A)u'_A(w_A - \pi_A c_A + c_A - L_{A4}) \\ & + (1 - d)(\delta_1 - \pi_A)u'_A(w_A - \pi_A c_A + \delta_1 c_A - L_{A5} + F_A)\}. \end{aligned}$$

In general this equation is a nonlinear algebraic equation which cannot be solved analytically. There are

however powerful and efficient numerical algorithms (available in most of the commercial computer packages) which deal with the solution of such problems. In the present paper we choose to treat a special case which allows for analytical treatment and provides some insight into the behavior of the optimal contract with respect to the relevant parameters of the model.

**Proposition 1** *Suppose that A has an exponential utility function of the form  $u_A(w) = D_1 - D_2 \exp(-\lambda_A w)$ ,  $\lambda_A > 0$ . Suppose also that the contract is such that  $\gamma_1 = \delta_1 = 1$ .*

- (i) *The optimal coverage for A is given by the positive part of the expression*

$$c_A = -\frac{1}{\lambda_A} \ln\left(\frac{\pi_A}{1 - \pi_A}\right) \times \frac{vp_1}{v\{p_2 c_2 + (1 - p_1 - p_2)c_3\} + (1 - v)\{dc_4 + (1 - d)c_5\}},$$

where  $c_i = \exp(\lambda_A L_{Ai}), i = 2, 3, 4, c_5 = \exp(\lambda_A (L_{A5} - F_A))$  and  $\pi_A = 1 - vp_1$ .

- (ii) *In the case where  $L_{Ai} = L, i = 2, \dots, 5$  the optimal coverage simplifies to*

$$c_A = L - \frac{1}{\lambda_A} \ln\left(\frac{\pi_A}{1 - \pi_A}\right) \times \frac{vp_1}{v(1 - p_1) + (1 - v)\{d + (1 - d)\exp(-\lambda_A F_A)\}}$$

*Proof* In the special case  $\gamma_1 = \delta_1 = 1$  the first order condition becomes

$$\begin{aligned} x(1 - \pi_A)\{vp_2 c_2 + v(1 - p_1 - p_2)c_3 \\ + (1 - v)dc_4 + (1 - v)(1 - d)c_5\} = vp_1 \pi_A \end{aligned}$$

in terms of the variable  $x = \exp(-\lambda_A c_A)$ . This is a linear equation for  $x$  which is readily solved. Upon inversion we get the proposed formula for  $c_A$ . In the case where  $L_{A2} = L_{A3} = L_{A4} = L_{A5} = L$  we factor out the common term  $\exp(-\lambda_A L)$  and yield the stated result.  $\square$

The following observations are in order. Consider case (ii). If furthermore  $F_A = 0$ , i.e., the fine paid by company B in case of proven fraud does not go to A, then substitution of the premium  $\pi_A$  in the above formula yields  $c_A = L$ . This is a very reasonable result, since A tries to cover for the whole possible loss just by insuring herself. If on the other hand  $F_A > 0$  then one easily observes that  $c_A < L$ . Thus the introduction of a compensation  $F_A$  paid in the form of a fine from B to A in case of fraud, lowers the optimal coverage of A

by I. In fact,  $c_A$  is a decreasing function of  $F_A$ . Again this result is very reasonable. Note also that for large enough values of the fine  $F_A$  the optimal coverage  $c_A$  may become zero.

One may further consider the effect of the probabilities  $d$  and  $\nu$  on the optimal coverage.

By straightforward algebra we obtain that

$$\frac{\partial c_A}{\partial d} = \frac{1}{\lambda_A} \frac{1}{\nu(1-p_1) + (1-\nu)\{d + (1-d)\exp(-\lambda_A F_A)\}} \times (1 - \exp(-\lambda_A F_A)) > 0$$

as long as  $F_A > 0$ . This shows that the higher the value of  $d$  is the higher the coverage asked from company A, i.e., the higher the probability of undiscovered fraud the higher the coverage asked by company A from the insurer. The coverage takes its maximum value  $c_A = L$  at  $d = 1$  and its minimum value

$$c_A = L - \frac{1}{\lambda_A} \ln \left( \frac{1 - \nu p_1}{\nu(1-p_1) + (1-\nu)\exp(-\lambda_A F_A)} \right)$$

at  $d = 0$ . This is a reasonable result since for high enough probabilities of discovery of fraud, company A expects the compensation  $F_A$  from company B except from the compensation from the insurer and so will ask for less compensation from the insurer in order to minimize the costs of the insurance contract.

We may also differentiate with respect to  $\nu$  to obtain

$$\frac{\partial c_A}{\partial \nu} = \frac{1}{\lambda_A} \frac{1}{1 - \nu p_1} \times \frac{1}{\nu(1-p_1) + (1-\nu)\{d + (1-d)\exp(-\lambda_A F_A)\}} \times (1-p_1)(1-d)(1 - \exp(-\lambda_A F_A)) > 0$$

as long as  $F_A > 0$ . This shows that the higher the value of  $\nu$  is, the higher the optimal coverage asked by company A from the insurer I. The optimal coverage takes its larger value  $c_A = L$  at  $\nu = 1$  and its smaller value

$$c_A = L - \frac{1}{\lambda_A} \ln \left( \frac{1}{d + (1-d)\exp(-\lambda_A F_A)} \right)$$

at  $\nu = 0$ . This again is a reasonable result since if fraud is impossible then company A will try to make up for the possibility of financial loss in an adverse state of the world by resorting only to the insurer, and thus try to insure for the full possible loss. If fraud is possible, but discovery of the fraud is also possible then the company may make up for the possibility of financial loss partially by the insurance contract and partially by the fine imposed on company B in the case of discovery of the fraud. Thus, company A will only insure partially, so as to save on the costs of the insurance contract.

*Remark 5* The assumptions of Proposition 1, i.e., the choice of the exponential utility function and the parameter values  $\gamma_1 = \delta_1 = 1$  are made only in order to be able to obtain analytical expressions for the optimal coverage. They are by no means restrictive; in fact, the results are expected to be robust with respect to different choices of the utility function or the parameter values  $\gamma_1$  and  $\delta_1$ , that reflect the terms of the contract.

### 5.2 The contract for B

The determination of the optimal contract for B is slightly more involved because of the incentive constraint. In the general case, the constrained optimization problem can be solved using the standard methodology of Lagrange multipliers, through the use of the Kuhn–Tucker conditions. The problem may not be solved analytically, in general, but fortunately there exist very efficient and easy ways to use numerical algorithms that can lead to the determination of the optimal coverage for B. However, for some special cases the problem may admit an analytical solution. We choose to present in this paper this special case, since the existence of an analytic solution allows us to gain considerable insight on the model.

**Proposition 2** Assume that  $u_B(w) = E_1 - E_2 \exp(-\lambda_B w)$ ,  $\lambda_B > 0$ . Assume furthermore that  $\gamma_2 = 1$ .

(i) The optimal insurance coverage by B is given by

$$c_B = -\frac{1}{\lambda_B} \ln \left( \frac{p_1}{p_2 C_2 + (1-p_1-p_2)C_3} \right)$$

as long as the inequality

$$d y C_4 + (1-d)y^f C_5 \geq p_1 + p_2 y C_2 + (1-p_1-p_2)y C_3$$

holds.

In the above

$$C_2 = \exp(\lambda_B L_{B2}), \quad C_3 = \exp(\lambda_B L_{B3}),$$

$$C_4 = \exp(\lambda_B G), \quad C_5 = \exp(\lambda_B F_A)$$

$$y = \frac{\pi_B}{1 - \pi_B} \frac{p_1}{p_2 C_2 + (1-p_1-p_2)C_3},$$

$$\pi_B = \nu(1-p_1) + (1-\nu)\{d - (1-d)f\},$$

(ii) In the case where  $L_{B2} = L_{B3} = L_B$  the optimal insurance coverage reduces to

$$c_B = L_B - \frac{1}{\lambda_B} \ln \left( \frac{\pi_B}{1 - \pi_B} \frac{p_1}{1 - p_1} \right)$$

as long as the inequality

$$y C_4 + (1-d)y^f C_5 \geq p_1 + \exp(\lambda_B L_B)(1-p_1)y$$

holds.

In the above

$$C_4 = \exp(\lambda_B G), \quad C_5 = \exp(\lambda_B F_A),$$

$$y = \exp(-\lambda_B L_B) \frac{\pi_B}{1 - \pi_B p_2 + (1 - p_1 - p_2)} \frac{p_1}{(1 - p_1 - p_2)},$$

$$\pi_B = \nu(1 - p_1) + (1 - \nu)\{d - (1 - d)f\}.$$

*Proof* We will look for an internal solution. In the special case  $\gamma_2 = 1$  the first order condition becomes a linear equation in terms of the variable  $y = \exp(-\lambda_B c_B)$ . This equation is readily solved to yield

$$y = \frac{\pi_B}{1 - \pi_B p_2 C_2 + (1 - p_1 - p_2) C_3} \frac{p_1}{C_3}.$$

Upon inversion we get the proposed formula for  $c_A$ . This is the solution to the problem as long as it satisfies the constraint. Upon substitution of the candidate for the internal solution in the constraint and algebraic manipulations we obtain the inequalities that must hold for the contract. In the case where  $L_{B2} = L_{B3} = L_B$  we factor out the common term  $\exp(-\lambda_A L)$  and yield the stated result.  $\square$

The following comments are due. First of all we see that the constraint always holds as long as the term  $F_A$  is large enough. So, if the contract is such that a large fine must be paid to A by B in case a fraud happens and is discovered, then there is incentive for B to act in a bona fide manner. A quick observation of the optimal insurance coverage yields that the decision on whether company B will be insured for more or less that the possible loss  $L_B$  depends on the probabilities of discovery of a possible fraud and the part of the fine that goes towards the insurer. More precisely we see that if  $1 - p_1 - d + f(1 - d) > 0$  then  $c_B > L_B$  whereas if  $1 - p_1 - d + f(1 - d) < 0$  then  $c_B < L_B$ .

*Remark 6* The assumptions of Proposition 2, i.e., the choice of the exponential utility function and the parameter value  $\gamma_2 = 1$  are made only in order to be able to obtain analytical expressions for the optimal coverage. They are by no means restrictive; in fact, the results are expected to be robust with respect to different choices of the utility function or the parameter value  $\gamma_2$ , that reflect the terms of the contract.

### 5.3 A case study

The main object of this work is to study the feasibility of adoption of insurance contracts for firms entering into some sort of outsourcing agreement. The aim of the insurance contract would be to cover company A from possible fraudulent behavior on the part of company B as well as from adverse states of the world where losses can occur by accidental reasons. To the best of

our knowledge such contracts do not exist and even if they do they are contracts based on mutual agreement between the companies involved and the insurer and as such there is not publicly available information on the contract terms. However, the present study can be extremely helpful first in proposing what the optimal terms of such a contract would be and second in showing that it is indeed beneficial for the company to enter such a contract. In the absence of insurance contracts of this type and thus of relevant data, we perform a simulation study, that will employ certain scenarios in order to assess the possible situations that may occur.

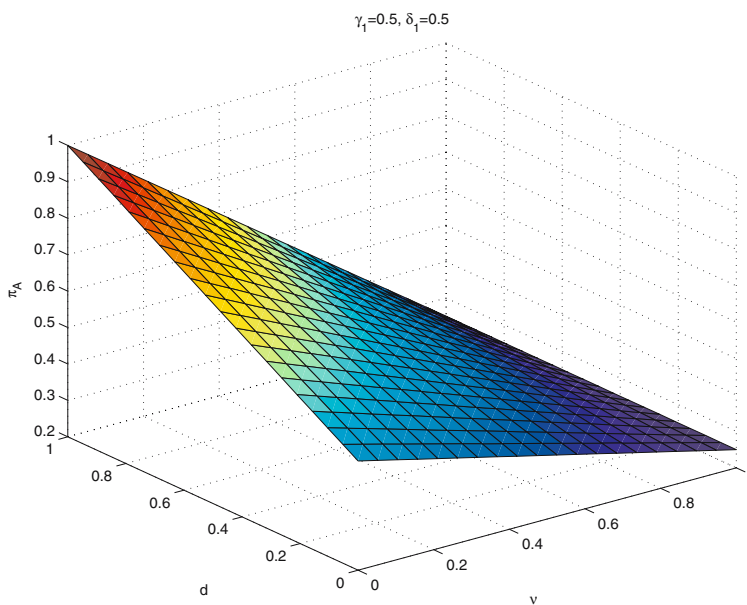
We first present some results on the premium of the contract for company A and for company B. The different scenarios, are related to the different possible values that the parameters  $\nu$  and  $d$  may take.

The premium for company A is shown in Fig. 1 for parameter values  $\gamma_1 = 0.5$  and  $\delta_1 = 0.5$  and in Fig. 2 for parameter values  $\gamma_1 = 1$  and  $\delta_1 = 1$ . We observe in both cases that the premium assumes its maximum value  $c_A = 1$  when  $d = 1$  and  $\nu = 0$ . This is very reasonable since this set of parameter values corresponds to the case where company B is very unreliable and given that fraud occurs it is highly unlikely to be discovered. In this case the insurer is likely to set the highest possible premium. On the other hand, the premium assumes its lowest value in the case where  $\nu = 1$  and  $d = 0$ . This is again very reasonable since this corresponds to the case that company B is very reliable and even if she commits fraud it is highly likely to be discovered. The premium in all other cases reflects a balance between the possibility of fraud and the possibility of discovery. Finally, we observe that as  $\gamma_1$  and  $\delta_1$  tend to 1 the relationship between  $\pi_A$  and the probabilities  $\nu$  and  $d$  is linear, whereas it is nonlinear for values close to 0.

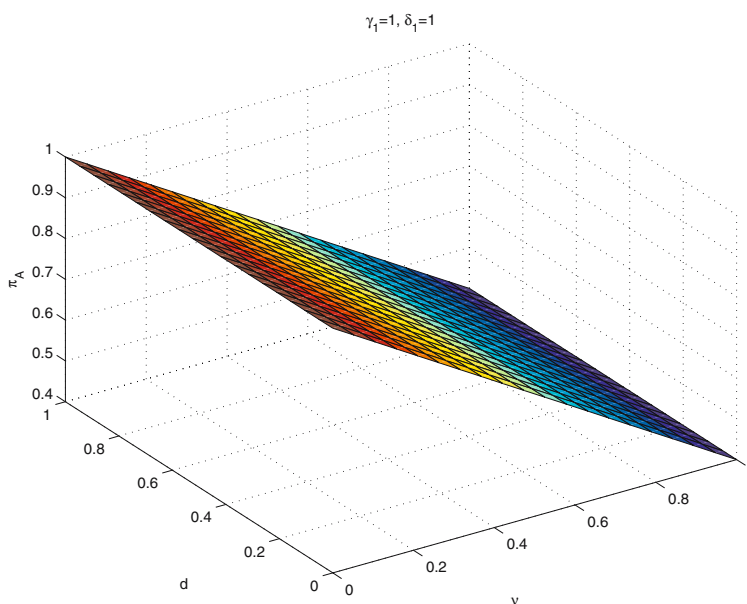
The premium for company B is shown in Fig. 3 for parameter values  $\gamma_2 = 0.1$  and  $f = 0$  and in Fig. 4 for parameter values  $\gamma_2 = 0.1$  and  $f = 0.5$ . It is first observed that the introduction of a fine payable from company B towards the insurer I, lowers considerably the premium for company B. This is understandable since the fine plays the role of a compensation towards the insurer in case of deliberate fraudulent behavior and as such reduces the risk taken by the insurer. We observe again that the highest values of the premium for B, are obtained when  $\nu = 1$  no matter what the values of the parameter  $d$  are. This is very reasonable since these parameter values correspond to the case of a very unreliable company B which is likely to cause deliberate losses and as such will be charged by high insurance premiums.

We next present some results on the optimal coverage by the insurance for company A. We focus on company

**Fig. 1** The premium for A,  $\pi_A$ , as a function of  $v$  and  $d$  for the parameter values  $\delta_1 = \gamma_1 = 0.5$



**Fig. 2** The premium for A,  $\pi_A$ , as a function of  $v$  and  $d$  for the parameter values  $\delta_1 = \gamma_1 = 1$



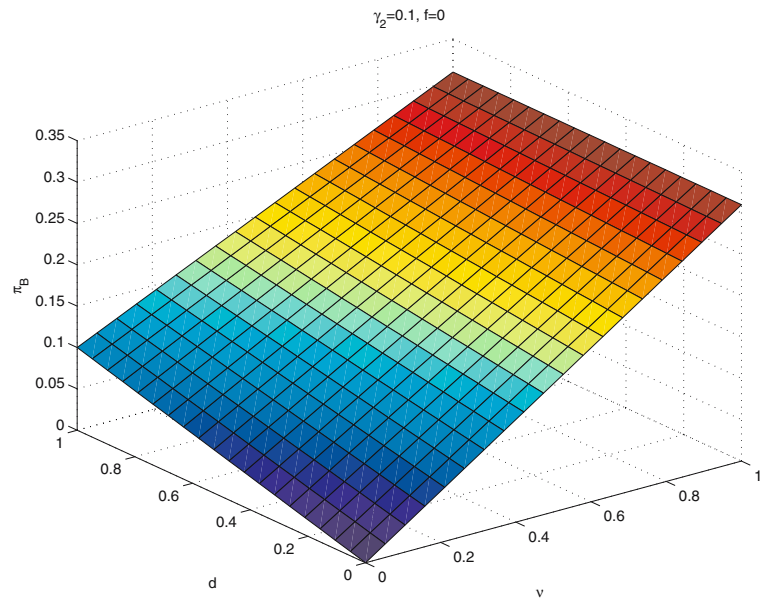
A since she is in the most vulnerable position, not knowing exactly what the intentions of company B are likely to be.<sup>1</sup>

In the first panel of Fig. 5 we present the optimal coverage per unit loss for company A, as a function of the parameters  $v$  and  $d$ , in the case where the risk aversion coefficient for A is  $\lambda_A = 0.1$  and when the fine paid by B to A in case of discovery of fraudulent behavior is  $F_A = L$  that is equal to the loss suffered by the company A. We observe that company A decides on maximal coverage in the case where  $d$  or  $v$  take values close to 1.

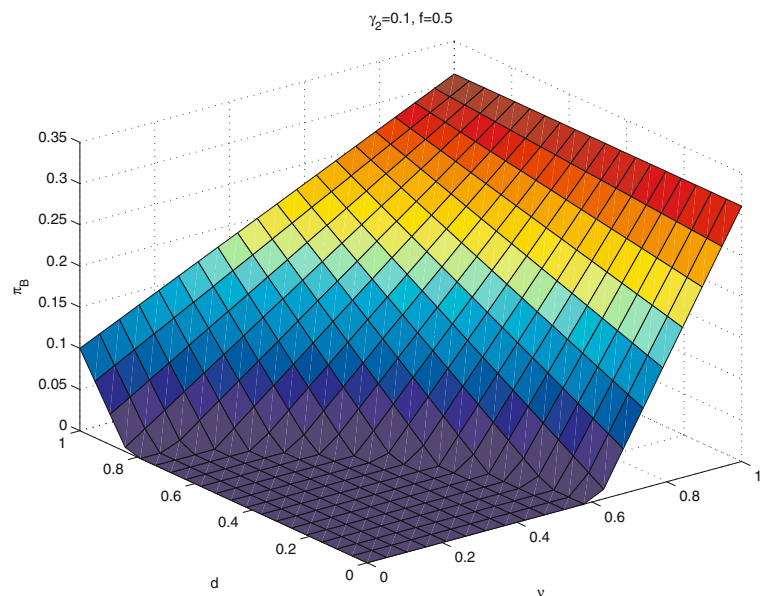
This is very reasonable since in the first case this set of parameter values corresponds to an unreliable company B that may commit fraud and if such a fraud occurs it is highly unlikely to be discovered and in the second case company A insures only against the states of the world, and since the insurance is actuarially fair she decides to insure for the maximum possible available sum. On the other hand the optimal coverage is low in the case where  $v$  and  $d$  take small values; this is again reasonable since this set of parameter values corresponds either to the case of a highly reliable company B or to the case of an unreliable company B but then fraud may be discovered and a fine will be payable that will compensate A. In the second panel of Fig. 5 we present the difference

<sup>1</sup> It is up to company's B discretion whether she will act in a bona fide way or not.

**Fig. 3** The premium for B,  $\pi_B$ , as a function of  $\nu$  and  $d$  for the parameter values  $\gamma_2 = 0.1$  and  $f = 0$



**Fig. 4** The premium for B,  $\pi_B$ , as a function of  $\nu$  and  $d$  for the parameter values  $\gamma_2 = 0.1$  and  $f = 0.5$



in expected utility for company A in the case where she decides to insure  $U_i$  and in the case she decides not to insure  $U_u$ . Eventhough expected utility is ordinal and not cardinal, this figure demonstrates that it is beneficial for company A to insure herself, even for low values of the risk aversion coefficient.

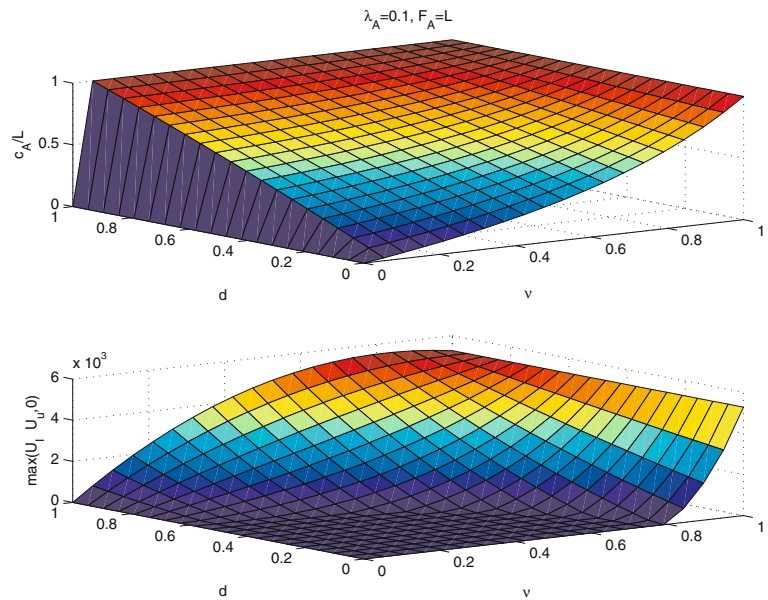
In the first panel of Fig. 6 we present the optimal coverage for A as a function of  $\nu$  and  $d$  again in the case where  $\lambda_A = 0.1$  but now  $F_A = 5L$ . Then we observe that the introduction of a higher fine payable to company A, reduces the optimal coverage by the insurer, for low values of  $\nu$  and  $d$ . This is reasonable, since this set of parameter values corresponds to the case where fraudl-

net behavior may indeed occur but it is highly likely to be discovered, so the fine payable by B will compensate A, therefore, she does not have to resort to insurance. In the second panel of Fig. 6 we present the utility difference for A which shows that it is beneficial for A to be insured for a given set of parameter values  $\nu$  and  $d$ . It is evident that as the parameter  $\lambda_A$  grows, the optimal coverage for A grows.

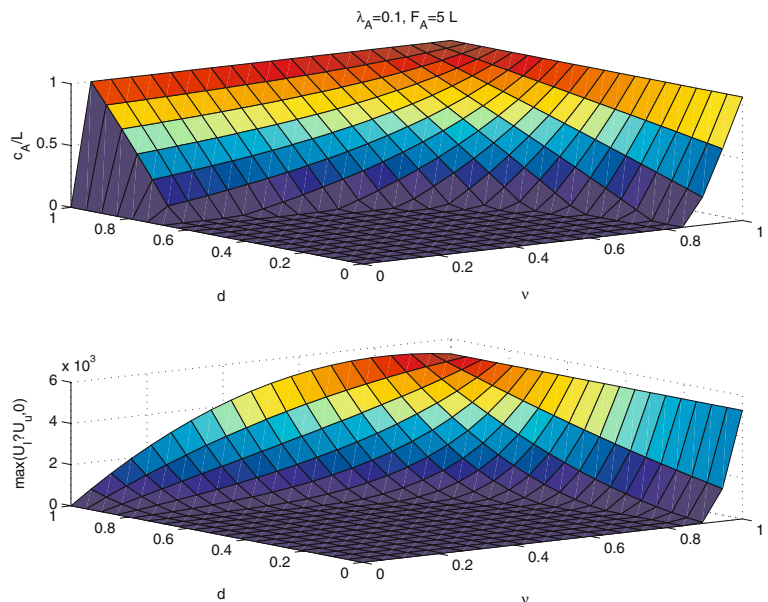
## 6 Generalizations and extensions

In this section we propose some interesting generalizations and extensions of our model. These extensions are beyond the scope of the present paper, however, they

**Fig. 5** The optimal coverage for A,  $c_A$ , as a function of  $v$  and  $d$  as well as the utility difference  $U_i - U_u$  for the parameter values  $\lambda_A = 0.1$  and  $F_A = L$



**Fig. 6** The optimal coverage for A,  $c_A$ , as a function of  $v$  and  $d$  as well as the utility difference  $U_i - U_u$  for the parameter values  $\lambda_A = 0.1$  and  $F_A = 5L$



are under active consideration by our research team and will be reported elsewhere in the near future.

### 6.1 Alternative premium calculation

There are alternative ways of calculating the premia that the insurance company will charge to companies A and B.

One way of calculating premia is in such a way so that I never loses no matter whether fraud occurs or not. For instance, one way of premium calculation would be to calculate  $\pi_B$  in such a way so that

$$\min\{E[G_B | \{1, 2, 3\}], E[G_B | \{4, 5\}]\} = 0$$

where by  $E[G_B | \{1, 2, 3\}]$  we denote the expected net gain from the transaction with B, given that one of the three states 1,2,3 occurs (no fraud) and by  $E[G_B | \{4, 5\}]$  we denote the expected net gain from the transaction with B, given that one of the two states 4,5 occurs (fraud). An easy calculation shows that  $\pi_B$  can be calculated by the solution of the equation

$$\min\{\pi_B - p_2 - \gamma_2(1 - p_1 - p_2), \pi_B - d\gamma_2 + f(1 - d)\} = 0$$

which gives

$$\pi_B = \begin{cases} p_2 + \gamma_2(1-p_1-p_2) & \text{if } f > \frac{d\gamma_2-p_2-\gamma_2(1-p_1-p_2)}{1-d} \\ d\gamma_2-f(1-d) & \text{if } f < \frac{d\gamma_2-p_2-\gamma_2(1-p_1-p_2)}{1-d} \end{cases}$$

This scheme of calculation of premia uses the fine in case of fraud as a method of lowering or raising the premia for B. With this scheme the insurer I, is more effectively covered. We may find that with this premium calculation scheme, depending on the value of the fine  $f$ , and the terms of the contract we may have cases where  $\pi_B > \pi_A$ .

It is interesting to observe that under this alternative premium calculation scheme, company B is insured for the whole loss,  $c_B = L_B$  if  $f > \frac{d-(1-p_1)}{1-d}$  whereas  $c_B < L_B$  in the opposite case.

Of course other possible premium calculation schemes may be possible. For instance we may consider a premium strategy set up by I so that the net gain from the transactions of both A and B are equal to 0 in the case of malicious behavior of B and in the case of bona fide behavior of B. We then get a system of two linear equations the solutions of which gives  $\pi_A$ ,  $\pi_B$ . However, in this case  $\pi_A$  and  $\pi_B$  are functions of  $c_A$ ,  $c_B$  a fact that complicates the solution of the optimization problem. In this scheme, the insurer I shares the risk of losses by possible fraud of B to both A and B. The complications introduced by this premium calculation scheme do not allow us to obtain an analytic solution to the model as before, however, the model is easily solved using numerical techniques. A more detailed study of different premium calculation scheme and the consequence of different policies on the choice of the optimal contract is beyond the scope of the present paper and is under active consideration.

## 6.2 Monopoly of the insurance market

An interesting extension of the model is to relax the assumption of a completely competitive insurance market. This assumption was used for the premium calculation throughout this paper, and led to premium calculation through setting the expected gain (either separately of A and B, or the total gain from the transactions by both A and B) of the insurer equal to 0. However, if the projects concerned are large projects, with large possible losses involved, and/or projects of a specialized nature it may be that only a few insurance companies are capable or willing to offer such insurance contracts. Therefore, we may have to consider a model where a monopolist insurer acts as a profit maximizer and companies A and B will have to comply to the insurer's offer. This is a model with a different philosophy which should lead to interesting results about the optimal contract.

## 7 Conclusion

In this paper we highlight the new threats introduced by the IT outsourcing business model, as well as how an insurance contract may be utilized by the outsourcing company for minimizing the consequences—financial or legal—that she may face in cases where an individual's privacy is violated under the responsibility of the contractor, either acting maliciously or not. Furthermore, we introduce a probabilistic model for determining the optimal insurance contract that can be applied to an IT outsourcing scenario. By optimal we mean that the insurance company can calculate, through the proposed model, the minimum amount for the premium of the contract, in the sense that she will neither enjoy any gains nor she will experience any losses. Specific generalizations and extensions of the proposed model are currently under investigation. Specifically we are examining alternative ways for calculating the premium as well as cases where the competition among the insurance companies is very low, or even non-existent, turning the insurer to act as a profit maximizer as opposed to the no-gain philosophy adopted in the paper.

**Acknowledgments** The authors wish to thank the anonymous referees for helpful comments.

## References

1. Acquisti, A.: Privacy and security of personal information: economic incentives and technological solutions. In: Camp, L., Lewis, S. (eds.) *Economics of Information Security*. Springer, Berlin Heidelberg New York (2004)
2. Anderson, R.: Why information security is hard—an economic perspective. In: *Proceedings of the 17th Annual Computer Security Applications Conference* (2001)
3. Aubert, B., Rivard, S., Patry, M.: Managing IT outsourcing risk: lessons learned. In: CIRANO Centre Interuniversitaire de Recherche en ANalyse des Organisations Scientific Series, 2001s-39 (2001)
4. Aubert, B., Patry, M., Rivard, S.: Assessing the Risk of IT Outsourcing. In: CIRANO Centre Interuniversitaire de Recherche en ANalyse des Organisations Scientific Series, 1998s-16 (1998)
5. Barry, E., Mukhopadhyay, T., Slaughter, S.: Software project duration and effort: an empirical study. *Inform. Technol. Manage.* **3**(1), 113–136 (2002)
6. Barthelemy, J.: The hidden costs of IT outsourcing. *Sloan Manage. Rev.* **42**(3), 60–70 (2001)
7. Basu, V., Lederer, A.: An agency theory model of ERP implementation. In: *Proceedings of the ACM SIGMIS'04, Tucson, USA* (2004)
8. Bodin, L., Gordon, L.A., Loeb, M.P.: Evaluating information security investments using the analytic hierarchy process. *Commun. ACM* **48**(2), 78–83 (2005)
9. Cavusoglu, H., Mishra, B., Raghunathan, S.: A model for evaluating IT security investments. *Commun. ACM* **47**(7), 87–92 (2004)

10. DiRomualdo, A.V., Gurbaani, V.: Strategic intent for IT outsourcing. *Sloan Manage. Rev.* **39**(4), 67–80 (1998)
11. Haberman, S., Pitacco, S.: *Actuarial Models for Disability Insurance*. Chapman and Hall, London (1999)
12. Gordon, L.A., Loeb, M.P.: The Economics of Information Security Investment. *ACM Trans. Inform. Syst. Secur.* **5**(4), 438–457 (2002)
13. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber risk management. *Commun. ACM* **46**(3), 81–85 (2003)
14. Gordon, L.A., Loeb, M.P.: *Managing Cyber-Security Resources: A Cost-Benefit Analysis*. McGraw Hill, New York (2005)
15. Keil, P.: Principal agent theory and its application to analyze outsourcing of software development. In: *Proceedings of the ACM EDSER'05*, St Louis, USA (2005)
16. Lacity, M., Willcocks, L.: Practices in information technology outsourcing: lessons from experience. *MIS Q.* **22**(3), 363–408 (1998)
17. Laffont, J.L., Martimort, D.: *The Theory of Incentives: The Principa-Agent Model*. Princeton (2002)
18. Lambrinouidakis, C., Gritzalis, S., Hatzopoulos, P., Yannacopoulos, A.N., Katsikas, S.K.: A formal model for pricing information systems insurance contracts. *Comput. Stand. Interf.* **27**(5), 521–532 (2005)
19. Odlyzko, A.: Privacy, economics, and price discrimination on the internet. In: *Proceedings of the 5th ACM International Conference on Electronic Commerce* (2003)
20. Richmond, W.B., Seidmann, A.: Software development outsourcing: contract structure and business value. *J. Manage. Inform. Syst.* **10**(1), 57–72 (1993)
21. Schechter, S., Smith, M.: How much security is enough to stop a thief: the economics of outsider theft via computer systems and networks. In: *Proceedings of the Financial Cryptography Conference* (2003)
22. Wang, E.T.G., Barron, T., Seidmann, A.: Contracting structures for custom software development: the impact of informational rents and uncertainty on internal development and outsourcing. *Manage. Sci.* **43**(12), 1726–1744 (1997)
23. Wu, D., Ding, M., Hitt, L.: Learning in ERP contracting: a principal-agent analysis. In: Sprague, R.H. Jr. (ed.) *Proceedings of the Thirty-seventh Annual Hawaii International Conference on System Sciences*, IEEE Computer Society Press, Los Alamitos, 2004 (2003)



**Prof. Athanasios N. Yannacopoulos** holds a B.Sc. in Physics from the University of Athens, Greece, and a Ph.D. in Dynamical Systems from the University of Warwick, UK. Currently he is an Associate Professor, and the vice-Chair of the Department of Statistics and Actuarial-Financial Mathematics, University of the Aegean, Greece. His research interests include Random and Deterministic Dynamical systems, Applied Stochastic Analysis, and Security and Privacy Economics.



**Prof. Costas Lambrinouidakis** holds a B.Sc. in Electrical and Electronic Engineering from the University of Salford, UK, an M.Sc. in Control Systems and a Ph.D. in Computer Science from the University of London, UK. Currently he is an Assistant Professor in the Department of Information and Communication Systems Engineering of the University of the Aegean, Greece. His research interests include Information Systems Security, Smart Cards, and Telemedicine Services.



**Dr. Petros Hatzopoulos** holds a B.Sc. in Mathematics from the University of Crete, Greece, an M.Sc. and a Ph.D. from the City University of London, UK. Currently he is a Lecturer in the Department of Statistics and Actuarial-Financial Mathematics, University of the Aegean, Greece. His research interests include Life Insurance, Actuarial Statistics, and Security and Privacy Economics.

## Author's biography



**Prof. Stefanos Gritzalis** holds a B.Sc. in Physics, an MSc in Electronic Automation, and a Ph.D. in Informatics all from the University of Athens, Greece. Currently he is an Associate Professor, the Head of the Department of Information and Communication Systems Engineering, University of the Aegean, Greece and the Director of the Info-Sec-Lab. His research interests include Information and Communication Systems Security and Privacy.



**Prof. Sokratis K. Katsikas** holds a Diploma in Electrical Engineering from the University of Patras, Greece, an M.S. in Electrical and Computer Engineering from the University of Massachusetts at Amherst, USA, and the Ph.D. in Computer Engineering from the University of Patras, Greece. Currently he is a Professor at the Department of Information and Communication Systems Engineering. His research interests include Information and Communication Systems Security and Privacy.