DIMITRIOS C. KOUMARIDIS
MASTER in APPLIED INFORMATION TECHNOLOGY
UNIVERSITY OF MACEDONIA – THESSALONIKI
2010

INFORMATION SECURITY ECONOMICS: An analysis for the impact of unsecure information in the enterprises.

ABSTRACT

In this essay we aim to present a really new subject, that of Information Security and specifically its economic consequences. It is a field with only one decade of history and researchers all over the world produce new knowledge everyday.

In our essay we present four different approaches on the subject that are connected to each other, some more and some less, but we give extra attention into outsourcing. A case study for the use of outsourced services can be used to find empirical data from within a company. After the presentation of the approaches we present statistical data that give us a quantitative dimension of the subject with an analysis in order to connect them with the proper approach.

We conclude our essay with an overview of our research, its limitations and by giving some research questions for future work.

INTRODUCTION

The main aim of the essay is to focus into different approaches of the subject. Along the research we managed to specify four different approaches of the subject from which we are going to focus mainly in one of them.

We start by presenting the four approaches and after that in the theoretical foundation we emphasize more into one of them in order to show the research being done from each researcher and their conclusions but mainly in one of them. These four different approaches are connected because they deal with the same subject but from different views each of them. We conclude by giving our own research questions.

We conclude with a case study concerning a greek insurance brokers company about the usage of outsourced services and their impacts. After this part we present our statistical data from which we give a quantitative tone in our essay. They help us understand the theory and boost us into our conclusion and gained knowledge.

LITERATURE REVIEW

The first approach is a research from Ta-Wei Wang [2] about the effects that disclosures have in business economics, regarding security policies and cases of security breakdowns.

The second approach from Christos Ioannidis et al [4] presents the "conflict" between systems administrators and systems users about confidentiality and availability. Also presents the endless effort of the administrators to exploit their budgets properly in order to rise their effectiveness.

The third approach on the subject from Ross Anderson [5] is more economic and less technical because security is a combination of technology and policy over the proper usage of it. It deals mainly with differences in sentiments over information security.

The fourth and last approach, in which we mention many researchers, deals with the rising development of the 3rd partner services in many businesses and the problems occurring from the adoption of this outsourcing policy from their side, especially mentioning that this way a business gives the opportunity to another company to process important and sometimes top secret data. With this last approach we are going to deal mainly in our essay.

THEORITICAL FOUNDATION

For a casual observer the four different approaches of the subject are not connected to each other, but for an experienced researcher there are links between them. While presenting each of the approaches, we will show how they are linked. We will continue by presenting them one by one.

According to Ta-Wei Wang [2], business nowadays relies heavily on information technology to perform daily operations. Because of this increasing reliance on information technology, information security related incidents could result in a tremendous impact on a firm's operation and significant financial losses. For example, a series of Denial of Service (DoS) attacks in 2000 resulted in online retailers and portals such as Amazon.com and Yahoo losing service for hours [7]. Also, the estimated average loss caused by security breach is approximately $290,000 US dollars per respondent in the CSI/FBI computer crime and security report in 2008 [8]. This evidence highlights the importance of information security to organizations which also raises organizational concerns about information security. In order to resolve the concerns and better manage information security risks, researchers and managers have strived to better understand and assess information security risks. For example, companies such as AOL Time Warner and Merrill Lynch have assigned a chief security officer to better understand security risks and to determine the resources needed to manage such risks [9].

He [2] also mentions that some firms announce risks related to information security publically. There are two competing motivations from the literature for why firms disclose risk factors. On one hand, the disclosure of risk factors may help reduce the uncertainty that investors have regarding the firm's performance [10]. On the other hand, a firm may disclose risk factors

in order to reduce its future litigation costs associated with adverse events [11].

In the information security context, either motivation may be valid. Some firms are inclined to disclose to indicate preparedness, which corresponds to the first motivation, whereas other firms disclose in order to head off lawsuits, which is the second motivation. Within Ta-Wei Wang's research, he examines the market's reaction at the time when the financial reports are released, to find out that there is a positive association between stock price and security risk factors disclosed in financial reports at the time when the reports are released (0.94, about a 2% cumulative abnormal return for a two-day window). However, the result is not significant which might result from the small sample size he took in his research for this type of regressions. The association was still positive even after considering whether the security risk factors are with or without action oriented terms. This positive association shows that firms with security risk factors are perceived to be prepared to future breaches (the first motivation in Introduction) regardless of the characteristics of the textual contents [12].

Ta-Wei Wang [2] through his research tries to examine furthermore investors' reactions to security breaches. Investors' reactions provide explanations to managers and researchers about what leads to the price and volume reactions to security incidents. When there is no disclosure cost, full disclosure exists because investors believe that nondisclosing companies have the worst possible information. However, if disclosure costs or uncertainty exist, companies will disclose only when the benefits exceed the costs. Disclosure may also be used to reduce ex post legal and reputation costs from bad news, or when the firm faces earnings disappointments.

He [2] shows how general market participants can adjust their investment decisions regarding breach announcements given the sophisticated investors' reactions. A trading strategy is performed to demonstrate profitable short-term investment opportunities given the information asymmetry among investors. He explores the association between the textual contents of the news articles about security breach reports and both the stock price and trading volume reactions to breach announcements. The results suggest that general breach announcements lead to different assessments of the impact of security incidents. However, specific news articles and those about confidential information result in a more consistent negative belief of the impact of security incidents on a firm's future performance. Interestingly, sophisticated investors do not react immediately to breach announcements. By taking advantage of the different perceptions among investors, we show that, on average, one can make about 300% annual profit around the breach announcement date.

The first approach can be connected with the following one because it has to do with costs, money generally and its effects in an enterprises' everyday performance. As we are going to notice furthermore during the presentation of the second topic, budgets always puzzle administrators because bad calls in their execution put their enterprises into trouble. The ideal equation is difficult to be found. But because most times cost tends to be more important than performance, security and integrity of the enterprises' systems are reduced. Cost reduction leads sometimes to third partners'

services and failures from their side leads to profit loss either directly or indirectly through disclosures in the press. On the other hand a disclosure for a major investment or update of an enterprise IT infrastructure will show that the administration is serious about information security.

In our second research subject we are focusing on the eternal problem between cost and performance. Christos Ioannidis et al [4] are dealing with the problem and it would be useful to present their work.

Information security and network integrity are issues of the utmost importance to both users and managers [19]. The cost of security breaches and fraud is considerable and such issues constitute growing concerns for policy makers, in addition to the legitimate concerns of the specialist technological community of experts. As the importance of networks increases for all individuals who act as both providers and consumers of information, the integrity of such systems is crucial to their welfare. In the presence of threats to the system, agents must decide the amount of resources required to maintain the system at acceptable operational states.

Finding solutions to this resource allocation problem is therefore an important part of the work of IT managers. As with all such decisions, expenditure in protecting a system has an opportunity cost because resources can be deployed for other useful purposes, a situation that requires the manager to demonstrate the desirability of such expenditure given an objective that takes into account that such protection costs are fully justified in the light of a well-specified objective.

The calculation of the optimal investment in information security given the system's configuration is a subject that focused almost exclusively on technological solutions without recourse to the associated financial costs and the behavioural changes required to implement such purely technological solutions.

The researchers [20] adopted an optimizing framework for the economics of information security, who provide an extensive list of references that address technological issues in information security and point out the distinct lack of rigorous economic analysis of the problem of resource allocation in information security. They adopt a static optimization
model where IT managers calculate the optimal ratio of investment in information security to the value of the expected loss under different assumptions regarding the stochastic process that generates the security threats. Within the framework of the model, we conclude that a risk-neutral firm should spend on information security just below 37% of the value of the expected loss that will occur in the event of breach.

The model relies on rather restrictive assumptions and has prompted lively debate regarding the 'optimal' ratio of investment in information security. What is of interest is that the relationship between investment in information security and vulnerability is not always a monotonic function. Other researchers [21],[22] are postulating an alternative functional form of vulnerability showing that the ratio cannot be supported and introduce the notion of the existence of a level of expenditure of information security that removes all threats, as an additional parameter, thus completely securing the information. Under this specification the 'optimal' ratio can vary according to the value of this parameter. The author constructs examples where optimal

investment ranges between 50% and 100% of the value of information that is protected.

As an example for these numbers referenced above, we can imagine the difference between the IT expenditure in a bank and a small industry that processes fruits. The IT department of the bank always tries to fulfill the ultimate task of 99,999% uptime which is the best possible nowadays. That means the bank's IT infrastructure can be out of service only 8 minutes time all over the year. It's a necessity for a bank to be almost everytime ready to serve every customer and employee within working hours or not. But that is not essential for other types of businesses like a fruit company. Having their systems 'of the net' for a few hours every year is not catastrophic. Here comes the difference in the IT expenditure between the bank and the other company. A bank will always pay more for IT security and integrity, because if it doesn't the losses will be tremendous either in real money or in fame and trust which sometimes is even worse than losing money. It has more to lose than to save by cutting the budget of IT security without a proper plan.

Finally we are going to present a different thinking on the subject which is more behavioural than technical. Differences in thinking and materializing of those thoughts leads to whole new equations between administration and IT professionals. Differences in thinking reduce or increase budgets according to the results they have.

The third approach is more theoretical, with a subject that deeply has to do with the human factor, the human attitude to be more specific. Ross Anderson [5], one of the pioneers in the field, is dealing with information security but he puts forward a contrary view than a technical one*:* information insecurity is *at* least as much due to perverse incentives. Many of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.

A characteristic example, referred by Ross Anderson [23], for the human factor and mainly the human behavior is the following one, concerning fraud against autoteller machines. In a survey it was found that patterns of fraud depended on who was liable for them. In the USA, if a customer disputed a transaction, the onus was on the bank to prove that the customer was mistaken or lying; this gave US banks a motive to protect their systems properly. But in Britain, Norway and the Netherlands, the burden of proof lay on the customer: the bank was right unless the customer could prove it wrong. Since this was almost impossible, the banks in these countries became careless. Eventually, epidemics of fraud demolished their complacency. US banks, meanwhile, suffered much less fraud; although they actually spent less money on security than their European counterparts, they spent it more effectively.

There are many other examples. Medical payment systems that are paid for by insurers rather than by hospitals fail to protect patient privacy whenever this conflicts with the insurer's wish to collect information about its clients. Digital signature laws transfer the risk of forged signatures from the bank that relies on the signature (and that built the system) to the person alleged to have made the signature.

In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected.

A different kind of incentive failure is Denial of Service (DNS) attacks. These exploit a number of subverted machines to launch a large coordinated packet flood at a target. Since many of them flood the victim at the same time, the traffic is more than the target can cope with, and because it comes from many different sources, it can be very difficult to stop [24]. While individual computer users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machines being used to attack Amazon or Microsoft [25].

A solution proposed is that the costs of distributed denial-of-service attacks should fall on the operators of the networks from which the flooding traffic originates; they can then exert pressure on their users to install suitable defensive software, or, for that matter, supply it themselves as part of the subscription package.

Closing the subject, we can assume that outlooks for information security are more subjective than objective. There isn't a common reference, especially in the behavior of major enterprises that depend themselves deeply in having their data secured.

Continuing with our last research subject, which is outsourcing, we can understand that it is really tight with the first subject, because the disclosure of such a strategic decision usually effects an enterprise positively or negatively. Positively because such a decision reduces the fixed costs of an enterprise by giving the effectuation of services somewhere else to a third partner, on the other hand gives the expression that the enterprise doesn't have strict security over the third partner which is generally a genuine assumption. Usually third partners that outsource services to others are secure enough, but it is not the same thing as to have every service and equipment within your own responsibility. That is why enterprises should always be really careful about their partners and keep checking their performance of the services they provide to them. A difficulty from a third partner, even a small failure that will last only an hour, sometimes has dramatic effects in an enterprise, because it will maybe stop its usual operation and when something stops functioning usually means losing money. And even worse losing face in the market is another effect that an enterprise has to fight hard to regain. A disclosure of such an event will effect both partners, the seller and the buyer, but the buyer can always buy from another provider. A low-quality service provider will not sustain competition for a long time. We will proceed by presenting the various researchers and their works on the subject.

Matilda Alexandrova [26] researchs outcourcing in South-East European countries. Outsourcing is not a new phenomenon in the world managerial practice but still rapidly develops establishing the beginning of a new stage of international division of labor. Outsourcing becomes a business practice through which the organization provides itself the possibility to mobilize its scarce time and financial resources and direct them to the development of its core competitive characteristics, in the same time achieving better results from its outsourced (secondary) business processes. Production relocation and offshore outsourcing of jobs in manufacturing

sectors have been occurring for decades in the world economy. Recently, along with the rapid technological development, investments in ICT infrastructure, ongoing trade liberalization in many service sectors and the availability of low-wage suppliers of skilled labor (like the new EU member states), outsourcing of services and particularly ICT-based business services, customer relations, back-office, and other professional services) has substantially expanded. In some sense, services outsourcing is qualitatively different from material outsourcing due to the easiness of border-crossing using new communication technologies such as the Internet.

There is no doubt that the main reason for the outsourcing decision is *costs* reduction. Organizations find that costs can be cut down by outsourcing of one or more business processes. An additional motive is to provide for a more flexible cost control. Foreign companies – e.g. clients of an outsourced service – have an option to react more adequate in case that the vendor makes attempts to overcharges them. A typical example for SEE countries is IT outsourcing targeted in cost reduction. It usually concerns software development operations performed by highly specialized personnel located in this low-cost environment. This efficiency effect implies a lower price of outsourcer's product which provides a better market positioning of the company.

The next study comes from Malaysia, a rising power in the field of outsourcing, especially in ICT outsourcing. Noor Habibah et al [27] made a research concerning ICT outsourcing in Malaysia's public sector.

In Malaysia, Information Technology and Communication (ICT) outsourcing practices are evolving as many organizations continue to identify its opportunities and benefits. This upward trend will likely keep growing as increasing fiscal pressures, citizen demands and workforce attrition drive both governments and public sectors to explore new operating models with embedded ICT technology.

An empirical study using a combination of questionnaire survey and interview was applied in this research. Both primary and secondary data were used in order to achieve this objective. Based on secondary data, risks inherent in ICT outsourcing were collected from previous research, mostly conducted in Kuwait, Spain and United States of America (USA). These inherent risks were used in this research to determine whether similar risks exist in the Malaysian public sector.

The research model, which is shown in the figure below, discusses the inherent risks in ICT outsourcing.

The twelve inherent risks are irreversibility of decision , ability to operate new system , lack of legacy and new system integration , lack of experience managing the outsourcing relationship , excessive dependence on outsourcer , the lack of outsourcer staff experience , the outsourcer not complying with the contract ,the hidden costs in outsourcing contract , unclear cost-benefit relationship , security (data confidentiality) , the loss of IT expertise , and the opposition of internal staff ,

Based on the twelve inherent risks, the research has formed the following hypotheses:

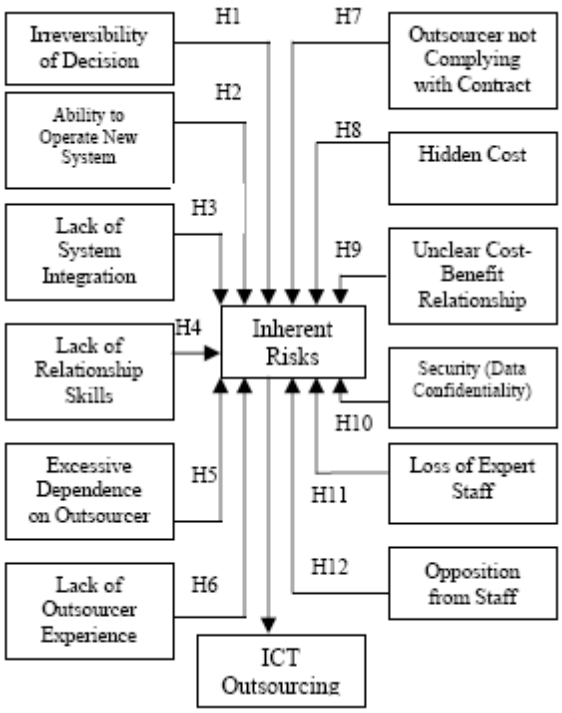


Figure: Research Model on ICT Outsourcing Inherent Risks

The highest mean in the next table represents the most outsourced ICT services while the lowest mean represents the least important ICT services outsourced in public sector organizations. The Malaysian government will allocate a total of RM12.9 billion on ICT. This amount is almost doubled that from the previous allocation of RM7.8 billion. Hence, a major portion of ICT allocation is on the computerization of government ministries and agencies with focus largely on supply and maintenance of computers and Internet access. This is indicative of public sector organizations moving forward to computerize more work processes and providing adequate support to its electronic government initiative. With more computers being used and better Internet access being provided, the need for network services increases. These network services are being outsourced largely due to the complexity of the tasks and the large number of tasks that need to be performed in the public sector industry. Among the important things related to the network service are the security and the speed of the network within the organization.

No.	ICT Services	Mean	Std. Deviation
1	Network services	61.1579	28.21585
2	Programming	59.9512	27.61648
3	Software maintenance	59.8305	26.31931
4	Hardware maintenance	57.0000	26.98787
5	System implementation	56.8786	26.27948
6	System operation	55.7723	32.00090
7	Application analysis	54.3440	24.84601
8	E-business solution	53.2763	27.29474
9	Security	50.6585	29.44621
10	Support end users	50.2846	26.71419
11	Staff/user training	49.2639	28.19115

Table: Ranking for the ICT services being outsourced

Continuing with the results on the hypotheses we come across some interesting findings. Pearson's Correlation Coefficient analysis was used to test whether there was positive relationship between ICT outsourcing and inherent risks. In order to test these hypotheses, the value of Pearson's correlation coefficient was calculated. Weak relationship is indicated by a value of less than 0.5, value between 0.5 to 0.7 indicate moderate relationship while a strong relationship has a value higher than 0.7.

Table: Association between outsourcing and inherent risks

	Pearson Coeff.	Sig.	Result
H1	0.724	.000*	High +ve relationship
H2	0.527	.000*	Moderate +ve relationship
H3	0.626	.000*	Moderate +ve relationship
H4	0.562	.000*	Moderate +ve relationship
H5	0.654	.000*	Moderate +ve relationship
H6	0.712	.000*	High +ve relationship
H7	0.748	.000*	High +ve relationship
H8	0.691	.000*	Moderate +ve relationship
H9	0.682	.000*	Moderate +ve relationship
H10	0.490	.000*	Weak +ve relationship
H11	0.632	.000*	Moderate +ve relationship
H12	0.495	.000*	Weak +ve relationship

**Significantce at 0.05 levels*

Results in the table above show that all the hypotheses (H1 to H12) were accepted where p-value < 0.05. The results however, indicated that H1, H6 and H7 have strong positive relationships. Based on the result of hypothesis H1, the assumption made is that public sector organizations may have experienced some loss when conducting ICT outsourcing due to irreversibility of outsourcing decision. Such a situation may happen when an organization is unable to ensure similar conditions before and after outsourcing. The possibility of some reversibility factor in ICT outsourcing decisions may need to be considered for public sector organizations especially if it pertains to, say, the organization's strategic IT. If by chance, that should be unintentionally outsourced, upon realization, reversibility could prevent further exposure.

Based on hypothesis H6 which was accepted, public sector organizations may have experienced situations where the results of outsourced activities are not as expected due to the lack of outsourcer staff experience in performing those activities. Even if some of the outsourcer had expertise in certain fields of ICT, there is no guarantee that they can handle a large outsourcing contract such as those from Malaysian public sector where projects are large-scale, diverse in nature and highly complex.

The result of hypothesis H7 indicated that public sector organizations may have experienced outsourcing results whereby the scope specified in the contract is not met. This could be due to the limited number of viable outsourcers in the market and high switching costs for the organizations if outsourcers did not perform. Many organizations in public sector have experienced outsourcer termination or interruption of contracts before all contractual tasks are completed and as a result organizations lose part of their investment on the contracts.

Surprisingly, hypothesis H10 has the weakest positive relationship. Apparently, the criticality of data confidentiality may not have been amply stressed by public sectors when they outsource their ICT activities. Information security should be an important issue in ICT outsourcing. The need for audit and control of data is of utmost importance because confidential and sensitive information about citizens are handled by many public sector organizations.

In general, based on the hypotheses, the table shows that even though some of the inherent risks are important, overall influence of the inherent risks to outsourcing activities is only moderate. Nevertheless, this result is consistent with previous literature, where ICT outsourcing has positive relationship with inherent risks.

Pertaining to the most common services being outsourced, network services was ranked the highest with outsourcers not complying with contracts being the most significant risk factor in ICT outsourcing. It is critical that organizations understand how to manage the risks that can contribute to ICT outsourcing failure. With effective risk management, the prime focus should be on planning to avoid future problems rather than solving the current problems. Moreover, by recognising and addressing inherent risks, organizations could improve the outsourcing environment. In this way, potential outsourcing organizations may be able to offer an additional incentive of a more secured outsourcing environment to prospective clients.

Nextly we are going to present a different approach that comes from within the education community. John S. Bojonny [28] made a research with a view of a professor , not for an industry but for a university’s campus everyday functions. Outsourcing has been around for years. There have been many variations of outsourcing over the years as well. IT executives view any discussion for IT outsourcing as an attack on their ability to manage and provide services to their clients. But dealing with IT outsourcing in higher education is more critical today than it ever was. And many campuses may already be doing some of this without even realizing it. Colleges that are financially pressed to streamline operations and generate revenue from other sources besides tuition are looking increasingly at outsourcing. One thing that is constant in considering outsourcing is that the responsibility for the function still remains with the institution and is not transferred to the outsourcer.

One might ask why an institution should consider outsourcing any of the IT functions. The changing playing field of higher education is one reason that IT outsourcing is important. With students now having more options to gain a higher education, they are demanding distance cources and distance services. More access to information via the Web is being demanded by students, faculty, and staff. Technologies are advancing too fast for the IT department to keep pace. Every facet of teaching is becoming dependent on technology. Institutions can no longer provide the computing capacity needed to perform the complex and high-computing-demand functions that research faculty are requiring. Managers are being pressured to reduce their baudets. Finding highly skilled IT staff is becoming harder and harder. And vendors are aggressively marketing these services and filling the gap. These are the pressures that are challenging campus IT departments. Because IT managers are being asked to find ways to reduce their budgets, the question will be not

whether an institution should consider outsourcing IT functions but rather when will all or some of the IT functions be outsourced.

One of the outsourcing options available is to outsource the entire IT function. This option is often considered when there is no existing management of the IT department or staffing is not adequate to provide all of the services needed by the institution. Outsourcing the entire IT department would require that the selected vendor staff the department. The outsource vendor might propose acquiring all of the equipment for a bargain price. The institution would then only have to pay the ongoing cost for the entire function being managed by the outsource vendor. When looking at the yearly cost for this it may appear to be a reduction in cost, because there are no capital costs that have to be budgeted for. And the institution would be paid money for the equipment. One caution in handing over all of the equipment to the outsource vendor is what happens if you want to switch vendors or bring the IT department back in house. The institution no longer owns the equipment, the vendor does. The capital costs would be significant. Another area to consider before making the decision to outsource the entire IT department, is all of the institutions knowledge of the applications that support the institution would be owned by the outsource vendor. Reacquiring that knowledge would also be costly and may not be possible at all.

When considering the options of outsourcing IT functions, there are certain functions that might make better sense to outsource than the entire department. Hard to find technical skills would be an ideal limited IT function for outsourcing. An example would be data base administration. There is a new variation of outsourcing an IT function. Net-sourcing involves paying licensing fees to application service providers or ASP's. This allows an institution to access browser based applications without the institution having to acquire equipment to run the application or install the software.

In conclusion, one thing to remember when considering outsourcing IT functions is that there is not a single solution for every institution. Each institution needs to ask what is being considered for outsourcing and why. And then make sure that all costs are considered, what are the true cost savings, institutional knowledge retention be taken into account, and what improvement will there be to customer service for the institutions students, faculty and staff.

David and Amy Chou [29] are focusing in an economic analysis of the software as a service (SaaS) outsourcing model. It is an emerging business model that delivers software applications to users through Web-based technology. Adopting SaaS applications allow companies to save their information technology cost.

Software as a Service (SaaS) is a newly emerging business model in the software industry. The growing speed of SaaS is fast. By 2011, 25 percent of new business software will be delivered as *Software as a Service*. The Internet is the backbone technology that provides life to SaaS business model. Just like Application Service Provider (ASP) model, SaaS can deliver software to user's computer and/or laptop for application processes. Although ASP and SaaS are similar in certain ways, their delivery models are different from each other. Other than that, service charges and financial revenues are diverse also.

Subscripting SaaS service will allow organization to save their IT investment on infrastructure, networking, hardware, software, and personnel costs. SaaS providers play the role of outsourcing vendors who offer the contracting service to their clients by charging a monthly fee. After that, SaaS providers will handle all needed services for their customers, including frequent application software's maintenance, customization, and updating. It is highly predictable that SaaS will win users' support in the near future.

Software as a service is a business model in the software industry that offering Internet-based software application programs to customers through the Internet channels and networks. Since customers just pay a subscription fee to rent the software for use, they do not need to keep the whole or partial application software in house. The scale of subscription fee depends on the number of users and the length of using time at customer's site. In essence, adopting SaaS software applications can save user's company a tremendous amount of IT expenses.

SaaS users gain the following advantages:

1. *Cost saving*: SaaS users can save a big portion of its IT operational cost by renting just needed applications for their business needs. The traditional IT expenses such as purchasing and maintaining hardware, software, infrastructure, and IT professionals could be minimized.
2. *Better resources utilization*: SaaS users can save IT expenses and then use the fund for more strategic processes.
3. *More application access scalability*: SaaS vendors frequently offer a multi-tenant architecture, which allows client side's application access to be scaled up or down immediately.
4. *Global outsourcing possibility*: The advancement of Web technology allows SaaS vendors to be located overseas and also offer the high quality services. The offshore outsourcing model allows SaaS users to save more IT expenses.

Adopting SaaS business model (i.e., pay-per-use charging) could save companies a tremendous amount of IT expenses. For companies intending to switch to SaaS setting, they need to assess the break-even point for existing IT investment, including the hardware, software, networking infrastructure, and even IT personnel. However, it is much easier for a start-up company to choose SaaS model for its IT capability since the investment in hardware, software, personnel, and complex networking infrastructure could be saved.

Selecting a SaaS outsourcing strategy would benefit the realignment of a company's organizational restructure and cultural change. However, this company must follow a series of stages to implement such outsourcing strategy. First of all, the top management must work with IT managers to determine their SaaS goals and then set the strategy. The second stage is to create the SaaS delivery model, including the search for a suitable SaaS provider. The third stage is to negotiate the SaaS contract with the targeted provider. The fourth stage is to identify needed service level agreements for providers' agreement. The fifth stage is to arrange and manage the transition in IT department. The sixth stage is to assign a project manager to work with the SaaS provider for maximizing the value of project and the harmony of working relationship. The last stage is to assess the outsourcing project through measuring performance of the project. The measurement results can be used to determine the likelihood of continuing such contract.

Apart of all the advantages Software as a Service has also some drawbacks, it's not a flawless outsourcing strategy. Data security is the main concern and growth obstacle for the SaaS industry. The future development of SaaS should focus on the design of data security and assurance for SaaS applications and transactions. Needless to say, customers will not subscribe SaaS service if they will not feel that their business data and transactions are securely protected by the vendor.

Since SaaS technology is still under developing stage, these are some issues need to be resolved before it can be fully utilized in the business world.

The next approach on outsourcing comes from outside the educational community but it would be useful to overview it. Jerry E. Durant [30] is Chairman Emeritus at The International Institute for Outsource Management so his research combines real data from the everyday processes in the enterprises. We are mostly interested for his view on the subject when things are going bad during outsourcing processes. There is always an element of risk. This is contributed by issues involving transitioning of operational culture from buyer to supplier. Factors involving the mode of operation, terminology, explicit and assumed expectations and general desires require formal transference to the supplier. The supplier then must make adjustments and adaptations in order to fulfill the delivery commitment while sustaining a stable operating environment within their company. The level of coordination and adaption is often underestimated. When failures occur it is blamed on culture and not on inattention to this important project administration point.

The first step to chipping away at these risks is to reflect on the level of project management involvement. Has proper care been given to,

- Correcting known deficiencies in artifacts, processes and operational involvement?,
- Established an orderly transitioning of duties from internal staff to external suppliers?,
- Developing sufficient checks-and-balances to retain continuity and control?,
- Adopting a 'buy right' vs. a 'buy large' attitude that insures viability and capability as cornerstones for select?,
- Clearly understanding governance responsibilities?, and
- Appropriately prepared for known contingencies (e.g. scope change)?

Contractual provisions help to arbitrary differences, and are essential, but do little to soften the effects of failed service delivery.

We will continue by presenting some interesting parts of a status report on Outsourcing of ICT and Related Services in the EU by Ursula Huws et al [31].

Nowadays telecommunications networks are capable of transmitting both voice traffic and any information which has been digitised, whether this consists of words, numbers, images computer programmes or any other data. This means that, in principle, any task that involves the processing of such material can be carried out remotely, using the telecommunications medium to receive and or deliver the results. Given the enormous spread of ICTs across virtually all sectors of the economy, this could, also in principle, mean

that a very large number, even a majority, of jobs could be outsourced offshore. In practice, there are a number of constraints on such large-scale relocation. In order to achieve a successful transfer, certain preconditions must be met. These include:

• Jobs are designed so that tasks requiring face-to-face contact are separated from those which can be carried out remotely
• The work to be transferred does not depend on tacit knowledge
• Tasks are clearly defined and standardised with performance measures enabling monitoring by results
• Well defined working procedures and quality control mechanisms are in place
• Good and clear communication patterns are in place
• Mutual cultural understanding and adjustment has been established
• A relationship of trust has been established
• Opportunities exist for face-to-face contact for conflict resolution and to ensure effective management and training.

In some circumstances additional constraints may come into play, including:

• Delocalisation outside national borders may be prevented by issues related to legal or professional liability
• There may be a reluctance to relocate high-value added, competition-sensitive core business activities (for instance, research and development) outside national borders. The development of a new economy has brought about a considerable convergence between economic sectors as traditionally defined, as well as giving birth to new sectors which are not yet separately identifiable in the existing statistics. It is thus no easy to task to identify those sectors in which offshore outsourcing is most likely to take place, or which portions of these sectors are likely to be affected.

In conclusion there must be a major preparation before taking such a decision to outsource, because it will affect almost every business process during the changes.

Furthermore into our research it would be useful to present the work being done on the subject from another non-academic source. Brent Rowe [32] of RTI International is asking whether outsourcing IT security can lead to a higher social level of security and also gives a thorough answer with the help of data from a study funded from the Department of Homeland Security (USA).

First of all we can identify ,according to his research, the several types of IT security outsourcing. IT security outsourcing relationships can take many forms, and as such, we provide here an overview of common types of IT security outsourcing relationships and types of MSSPs. Organizations can outsource six main technical tasks:

(1) penetration or vulnerability testing, (2) security auditing, (3) system monitoring, (4) consulting, (5) forensics, and (6) general system management.

Firms also outsource legal assistance and insurance to protect against potential liability issues or major losses associated with cyber events. The 2006 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey found that 61% of firms outsource no IT

security services. While technical definitions differ slightly, our study for DHS found that approximately 72% of firms do not outsource monitoring activities, the term most aligned with the CSI/FBI definition of IT security services.
The least intrusive outsourcing is *vulnerability testing*; under such an agreement, an external firm is hired to attempt to break into a company's network and identify areas of vulnerability. Our data collection for DHS found that approximately 58% of organizations outsourced vulnerability testing. The CSI/FBI survey found approximately 66% conducted penetration testing, though they do not indicate the percentage of such activities that are outsourced. It would seem that hiring someone external to attempt to break into a network would be much more effective than having someone who works on the network, and has detailed knowledge of the system configurations, conduct such an exercise. However, outsourcing this service can cost between $12,000 and $15,000.

Security auditing entails a comprehensive assessment of security hardware, software, policies, and procedures. In the CSI/FBI survey, 62% of firms reported that they hired external security auditors the previous year. Usually this type of service is conducted once or twice per year. It allows an organization to get a "report card" from an external firm based on an extensive assessment of the security measures in place. Using an external firm ensures that firms benefit from knowledge of both successful and unsuccessful solutions being employed at other firm; this information would be acquired by MSSPs from previous clients, but may not be as accessible to internal auditors.

System management is when a firm is hired to fully manage the firewall, virtual private network (VPN), and intrusion detection hardware and software protecting a company's network activities. This is the most intrusive form of security outsourcing. In a 2002 article in *IEEE Computer Magazine,* The management of a company firewall, VPN, and intrusion detection infrastructure is "too central" to a company's operation for it to be efficiently and effectively outsourced. There is no profitable business in managing
firewalls or, more broadly, managing network security for other companies, and he points to past relationships in which companies outsourcing such activities have demanded too much individual attention for the money they were paying. Companies should outsource firewall management, as well as several other functions that generally support the management of network security—intrusion detection and prevention, patch management, antivirus, and vulnerability assessment.

Type of Outsourcing	Percent
Purchase third-party insurance	22.2%
Monitoring of IT security issues	27.8%
Installation, implementation, and/or maintenance	52.8%
Vulnerable assessment/planned compromise	58.3%
Security auditing	62.0%[a]
Purchase legal consultation (internal or external)	63.9%

Table: Percentage of companies tha outsource

System monitoring, consulting, and *forensics* are all less intrusive than system management. A firm can be hired to perform 24/7 *monitoring* and interpretation of system events throughout the network, including unauthorized behavior, malicious hacks, denial of service (DOS) attacks, anomalies, and trend analysis. We found that only 28% of companies outsource security monitoring. In talking with several of the firms that do not outsource security monitoring, we heard anecdotal evidence of very costly (and unsuccessful) attempts at outsourcing monitoring in which it became apparent to the firms that the upfront transactions costs were going to be too high (in dollar terms and time) to achieve the short- or medium-term savings that were desired. Consulting and forensics services are also offered by many MSSPs.

Consulting relationships involve hiring an outside firm to help provide general or specific advice on security purchases or practices. Forensics services are usually employed to help find a specific problem or track how and why someone was able to breach a network. Based on the type of outsourcing relationship, costs and benefits will differ significantly.

Nextly we have tables with interesting statistics on the field.

Company Type	Installation, Implementation, and Maintenance	Monitoring of IT Security Issues	Vulnerable Assessment/ Planned Compromise	Purchase Third-Party Insurance	Purchase Legal Consultation (Internal or External)
Financial	50.0%	50.0%	100%	50.0%	83.3%
Health care	66.7%	0%	33.3%	33.3%	66.7%
Manufacturing	83.3%	33.3%	66.7%	0%	50.0%
Other	40.0%	20.0%	80.0%	40.0%	60.0%
Small business	66.7%	66.7%	66.7%	16.7%	66.7%
University	14.3%	0.0%	14.3%	0%	57.1%
Average	52.8%	27.8%	58.3%	22.2%	63.9%

Table: Percentage of Companies That Outsource, by Industry

Company Type	Outsource Something (1 of 5)	Outsource Installation, Implementation, and Maintenance, or Vulnerable Assets (1)	Outsource Installation, Implementation, and Maintenance, or Vulnerable Assets (2)	Outsource Installation, Implementation, and Maintenance, or Vulnerable Assets (All 3)
Financial	100%	100%	50.0%	50.0%
Health care	83.3%	66.7%	33.3%	0%
Manufacturing	100%	100%	50.0%	33.3%
Other	100%	100%	20.0%	20.0%
Small business	100%	83.3%	66.7%	50.0%
University	50.0%	14.3%	14.3%	0%
Average	83.3%	62.5%	58.3%	37.5%

Table: Percentage of Companies That Outsource One, Two, or Three Functions

Outsourcing has many benefits for a company that chooses to adopt it, especially economic benefits. But all types of outsourcing can be quite risky and can involve many costs. The most often discussed risk related to outsourcing is usually the effect of the principal-agent problem; which exists when the incentives of an individual in a management role at a firm are not aligned with the interests of the owner or shareholders of the organization. For example, a CEO who does not receive stock in his company might not be as concerned with how his actions affect the share price.

Similarly, a manager at a small business who does not get some share of the profits may not try to reduce costs or boost sales through extra effort or more efficient work. In the area of IT security, the principal-agent problem is even more difficult because it is very hard to tell how much effort the MSSP is exerting. Security problems likely will result at most firms even if their MSSP has aggressive security measures in place, and as such, the outsourcing firm might not realize if the MSSP is shirking or not performing their service at the level claimed. As a result, the incentive for MSSPs to shirk is quite high. However, outsourcing still occurs, so presumably MSSPs must not shirk much or else their shirking cannot adequately be observed and firms that outsource are not aware of the true extent of shirking.

Shirking can be mitigated by several factors. An open flow of information about service quality and appropriate assignment or distribution of liability can both help. As mentioned above, the first solution is very difficult to employ with respect to IT security outsourcing activities. The IT security environment changes frequently (i.e., new types of attacks emerge), and the time to monitor the service being provided could at least partially negate the benefits (cost savings) being sought by a firm. However, an MSSP's reputation, though not likely based on explicit knowledge of the firm's actual activities, can provide at least some measure of motivation for firms not to shirk. If a firm is thought to be shirking, the effect on their business could be extreme, and as such, it may not be worth the risk for them to shirk to any significant degree.

Liability alignment, however, could help. The establishment of strict liability in outsourcing relationships would mean that the MSSP would be fully liable for any successful attacks on one of their customers. This paradigm is not likely to exist because of the constantly evolving nature of security attacks means that some successful attacks will almost certainly occur. Negligence is when a firm is held responsible if they do not provide "adequate" security—standard of care—as determined by a contract and a court of law.

In the past, MSSPs have not borne much if any liability for security breaches. MSSPs generally state in their contracts that they cannot identify all incidents, and as such, when an incident does occur, they are not liable for the damages. A still open question for debate is whether the legal system could help realign liability issues concerning IT security events. With change in the legal system and if there is a significant lack of information about the quality of service being provided by MSSPs, the percentage of firms outsourcing IT security may not increase significantly in the short-run.

A multitude of additional risks are involved in IT outsourcing, many of which are shared with other types of outsourcing relationships. A working paper discusses two additional types of outsourcing risks:
potential theft of propriety information and postcontractual renegotiation. In the case of IT security, the MSSP could steal proprietary information (referred to as “poaching”) from its customers and sell this information to competitors. The MSSP could renegotiate the price of its contracts with customers after the outsourcing firms feel locked in; this is often called postcontractual renegotiation, or opportunistic repricing, and it occurs when a firm decides to raise its price after its customers have invested in setting up the relationship and are unlikely to enter into a new relationship.

Outsourcing also involves explicit costs that appear in some form or another regardless of the riskiness of the relationship. Most significantly, transactions costs and interoperability costs with an MSSP can be quite high. MSSPs often establish a slate of security packages that address different company characteristics and needs, but firms differ in many ways that cannot always be considered prior to the initiation of a relationship. Firms differ in the ways in which they use the Internet, the sensitivity of their data, the regulations with which they must comply, and the management oversight of their security. Additionally, when information (e.g., data on access and breaches) needs to be transferred, interoperability problems are likely to result. As such, at the beginning of and at periodic times throughout every outsourcing relationship, there will be an upfront investment required to minimize transactions and interoperability costs throughout the term of the relationship.

The main “losers” in IT security outsourcing will be IT security staff who work onsite at companies who decide to outsource their security activities. Although outsourcing doesn’t necessarily mean a net societal loss of security jobs, it does imply a shift from one position, for example at a manufacturing firm, to another position at an MSSP. For the security director or manager at the manufacturing firm, cost per unit of security is the motivating factor in making the decision to outsource or not. However, using the same example, security staff at the manufacturing firm have an incentive to explicitly suggest or imply that the costs to outsource will be higher and benefits will be lower than will actually be the case during and after the transition to outsourced security services, assuming outsourcing will result in some layoffs at the manufacturing firm.

It is useful to observe a different point of view from a non-profit organization like RTI International because it combines academic knowledge with real world data and that combination gives us interesting conclusions.

Zach Zhou with Eric Johnson [3] are also among the researchers that work on the problem of security breaches because of outsourcing. There have been several recent efforts to develop a common reference for rating the information risk posed by partners. They developed a simple analytical model to examine the impact of such information security ratings on service providers, customers, and social welfare.

They [3] mention that outsourcing has been widely adopted in many industries. Within the IT function, the benefits of subcontracting specific technology services and entire business processes include cost reductions, improved utilization of core IS resources, and the acquisition of new technical skills and competencies [13]. Recent technology innovations allowing increased network bandwidth, processing virtualization, and inexpensive storage have pushed outsourcing to a new level by facilitating the migration of many internal IT applications to externally provided services.

In this so called Software as a Service (SaaS) model, business applications are provided on demand as a service to customers. SaaS allows firms to reduce many fixed costs associated with the required internal IT infrastructure, application deployment, testing, maintenance, and patch management. It also lowers cost through competition. While these different forms of outsourcing provide enterprise customers with both flexibility and cost benefits, the use of external service providers handling sensitive business data introduces new security risks [14]. Many widely publicized security breaches have been the result of a partner failure. Sometimes these failures stem from neglect or under-investment in security. In other cases, the security challenges arise from the nature of the service provider's business model. Providers, who frequently enhance their service offering in response to evolving customer demand, introduce the possibility of new security bugs with every additional feature. Traditional methods in software assurance, with significant code testing, can be time consuming, slowing the vendor's ability to compete and tempting them to cut corners.

Of course a second worry is the firm's sensitive data that may be stored on a provider's machines and handled by employees of the service provider. That data represents a significant risk because the firm no longer has the ability to directly monitor and control its access. Even if the vendor's network is secure, the firm faces many web-based threats (hacking, malicious code etc.) when data is moving from the provider's facility over the Internet. Lastly, service providers often employ a model of multi-tenancy, where many enterprise customers share the same business application infrastructure with controlled access to their own data. The challenge for such a provider is segregating the customers' data. Inadequate data management may allow one firm's data to be exposed to another customer, which may be a competitor in the same industry.

For all of these reasons, firms must assess the information security level of their partners. Traditionally, customers perform such assessments through surveys, interviews, on-site visits, testing, and document review. Using that information the customers typically develop their own risk

assessment (through identification of threats and vulnerabilities, control analysis, likelihood determination, risk determination etc). [15]. This is timeconsuming and costly for both vendors and customers. Since many firms (especially those in the financial industry) have hundreds of service providers, the time required to perform the risk assessment can make it impossible to assess every critical service provider.

Recently there have been several efforts to develop a common risk rating. The idea behind such ratings is to reduce the burden for both enterprise customers and service providers by creating a single risk rating that can be efficiently used by many (rather than each firm individually assessing each of their vendors). [16]. While it is tempting to directly equate information security rating with ratings of financial instruments, security ratings are quite different from credit ratings (which measure the default probability for a debt issuer). A good credit rating generally enables the debt issuer to raise money from the financial market at a lower cost [17]. However, a good security rating does not necessarily benefit a high-security service provider because the security rating may have subtle impacts on the competition among service providers, their incentives to improve security levels, and their prices charged to customers.

Zach Zhou with Eric Johnson [3] through their research are trying to answer some demanding questions like whether risk rating always benefit the high-security service provider (or hurt the lowsecerity service provider). If not, how does risk rating affect different service providers under different market conditions? Another of their concerns is whether risk rating always benefit the most demanding customers who desire highly secure business partners? And lastly does risk rating increase social welfare?

They [3] developed some very interesting results. While it is commonly believed that information security rating benefits high-security service providers (and conversely hurts low-security providers), they found that, surprisingly, information security ratings can hurt or benefit both types of service providers, depending on the market conditions. This occurs when the absence of a security rating softens competition allowing the low-security service provider to appear identical to the high-security service provider. In that case, the low-security provider is able to charge a higher price than otherwise and the high-security service provider is able to avoid providing a positive net surplus to the high-type customer to guarantee that the customer does not choose the lowsecurity provider. Therefore, it is possible that the information security rating can intensify competition and hurt both service providers. On the other hand, in some cases information security ratings can benefit both service providers. For example, in cases where the hightype customer is not significantly different from the low-type customer, it is useful for both service providers to differentiate their services though security to avoid head-to-head price competition. Since ratings clearly reveal the security of providers, such information helps service providers differentiate themselves and thus can benefit both.

While prior literature [18] showed that improved information always benefits the high-type customer their model [3] shows that information security ratings can hurt the high-type customer. This is because their model captures competition between heterogeneous providers while prior researchers assumed homogeneous providers where profit is competed away. They found

that information security ratings have subtle effects on the competition. When the rating is provided, it may reduce the low-security service provider's incentives to invest in security. This reduces the quality of the alternative choice for the high-type customer. Thus, the highsecurity service provider will not need to provide a large net surplus to lure the high-type customer. This explains why the high-type customer can be hurt by an information security rating of providers.

Although the information security rating has subtle effects on service providers and customers respectively, it always increases the social welfare. The policy implication is that information security rating should be encouraged by social planners.

As we noticed there are connections between the different approaches because information security has to do with technology, economics, human behavior, differences in sentiments, so it's not something unidimensional. It can be viewed from many aspects. That is why problems about information security are not unilateral and can be solved only after cooperation from people in those different fields we have just referred.

It would be useful to set some research questions for the readers that could help them continue their own work on the subject furthermore.

First of all because of the really few years of research, does the academic community, especially in IT, has a real concern on the subject or we are still in start level? We have just passed the first decade of activity on the subject and still, especially in developing countries information security is not a real concern or it's in the hands of IT managers without a real security policy from the administration.

Another question that supplements the first one is whether enterprises are aware of the real dangers that accompany the handling of information, especially in eras when laws about information handling and information security are getting really tough?

Does the academic community understand the combination of two different sciences in the field of information security economics? It's neither a strict IT subject nor an economic one.

And finally about the main research subject, that of outsourcing, because of the continuing increase in IT outsourcing adoption from the enterprises, is there a simultaneous increase in the dangers because of it or there is an understanding from the enterprises' side about those dangers and efforts to deal with them?

CASE STUDY

It is always useful to present data from the everyday function of a company. We will present the view on the subject of Infotrust's SA IT administrator. I would like to thank especially Mr.Alexandros Vergidis for his time, helping me fulfill the task of this case study.

Infotrust SA is an insurance broker company situaded mainly in Thessaloniki, Greece with two other branches in Athens and Rhodes. It functions between insurance advisors and insurance companies and of course there is a need for electronic communication and data handling. The company separates the two functions. It keeps the clients personal data within its own infrastructure, within its own servers but it outsources its crm (customer relationship management) system from another company using Software as a Service.

Nextly there is a questionnaire with answers from the company's IT administrator.

QUESTION	YES	NO
1) Is the outsourcing decision irreversible?		✔
2) Are you able to operate the new system?	✔	
3) Does the system lack in integration?	✔	
4) Is there excessive dependence on outsourcer?	✔	
5) Does the outsourcer lack in experience?		✔
6) Does the outsourcer comply with the contract?	✔	
7) Any Hidden costs?		✔
8) Is there any unclear cost to benefit relationship?		✔
9) Are the data secure? (confidentiality)	✔	
10) Any specialized equipment needed for the operation of the CRM?		✔
11) Would it be possible to have the same level of services from within the IT department with the same cost?		✔
12) Are clients personal data involved in the systems transactions or kept within the premises of the company?		✔
13) Are you satisfied from the everyday support from the outsourcer? (debugging ,development etc)	✔	
14) Any loss of expert staff because of outsourcing?	✔	

We can combine the given answers with the following data. The number of company's employees are 40, so 40 licences (e-mails) are needed at least. Each licence costs 30 € per month so there is a cost for the company just from the usage of the crm around 1200€ per month and almost 15000€ per year. But if one puts it against the cost of a fully manned IT department with many employees and equipment it is better of course to outsource all these services.

One major issue for these kind of services is whether a contract exists between the company and the outsourcer about when the services are not fulfilling what the outsourcing company wants to receive. In this occasion such a contract exists and says that the service is available 24 hours per day / 7 days per week. When problems occur the outsourcer should reply to the notice within 4 hours and fix it, give a solution within 48 hours.

As we can notice, in small and medium-sized businesses it is better to outsource activities of the IT department from somewhere else but only after thorough search of the market, because the ideal balance between the benefits and dangers is difficult to be found. In the case study's paradigm personal data are not handled via an outsourced service. But it is always an administration decision.

STATISTICAL DATA

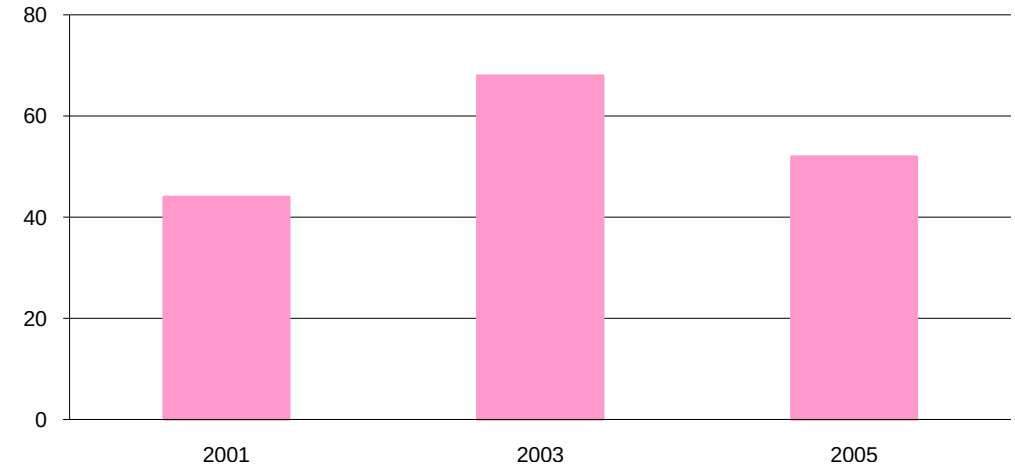
Simultaneously with the presentation of four approaches in information security, we will combine them with statistical data taken from the United Kingdom's Office for National Statistics [6]. We will use a 2007 report named: "Focus on the Digital Age'' which gives an overview of the digital age across society and economy in the UK. It shows the extent to which people, education, business and government have taken up information and communication technology (ICT), and how it is changing leisure, working and business practices. It also compares the use of ICT in the UK with that of other countries and analyses some of the problems associated with the digital age.

We will show some interesting graphs and data selected from the report and explain how each of them is combined with the approaches on the subject mentioned previously. Some of them are data concerning economic consequences of electronic crime, others about investment and policies in the field of information technology and some about the types of electronic threats that a business has to counter nowadays. From the data the reader may make various assumptions about the complexion of the subject and the consequences it produces

Businesses that had a malicious security incident (during a year)

United Kingdom

Percentages



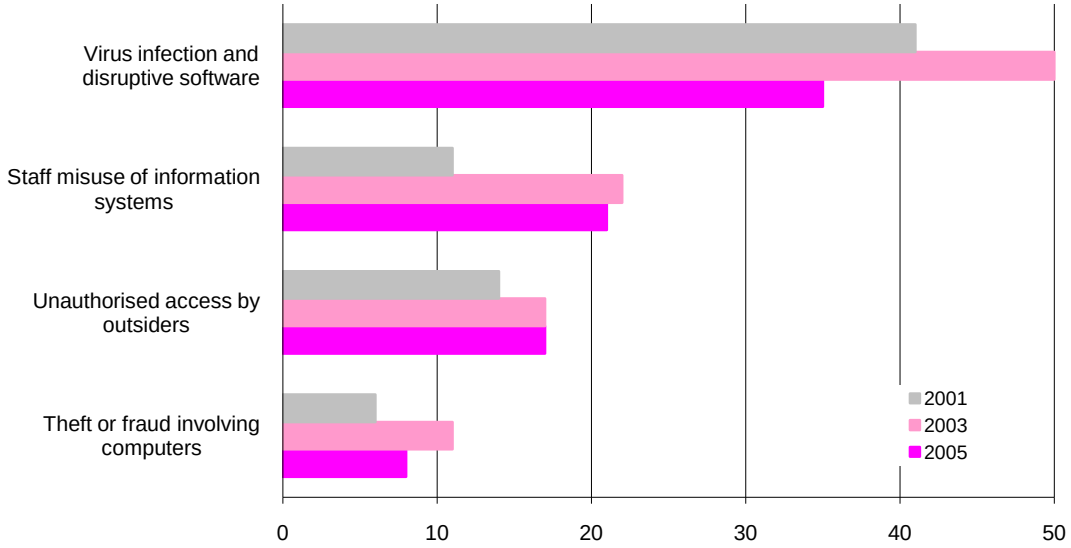
Businesses that had a malicious security incident (during a year)

United Kingdom	Percentages
2001	**44**
2003	**68**
2005	**52**

Graph – Table 1: Businesses that had a malicious security incident , in general.

We can understand from the graph above that nearly one out of two businesses, in the UK, had a malicious security incident in 2001, a percentage that exploded to 68% only two years after and only descended to 52% in 2005. The percentage is huge if we think that UK is already a developed country with high-tech businesses established in the country, so it is a matter that we can combine with the first and last approaches of the subject that refer to policies and impacts of information security, especially when security is breached.

Businesses suffering a malicious e-security breaches: by type of incident
United Kingdom
Percentages



Businesses suffering a malicious e-security breaches: by type of incident

United Kingdom			Percentages
	2005	2003	2001
Theft or fraud involving computers	8	11	6
Unauthorised access by outsiders	17	17	14
Staff misuse of information systems	21	22	11
Virus infection and disruptive software	35	50	41

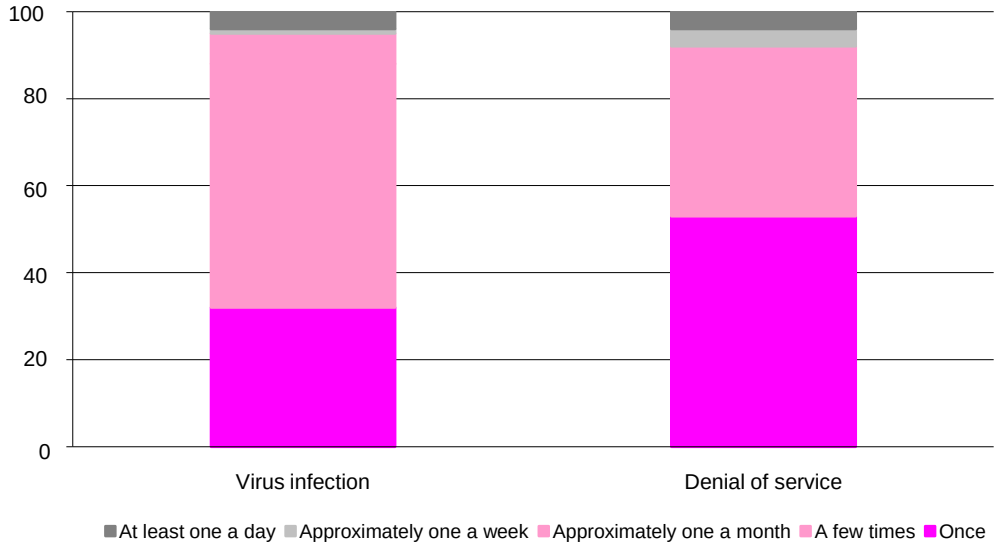
Graph - Table 2: Entreprises' percentages suffering malicious e-security breaches by types of them.

The graph above gives us knowledge for the extent of e-security breaches by type of incident which is useful, because we recon an increase in most types of incidents from 2001 to 2005 and in one case, that of information systems misuse, an increase of nearly 100%. Misuse from the staff nearly doubled in an era when information technology worldwide entered almost every kind of business. This is more important for a country like the United Kingdom because there is already huge experience in the field. Misuse first of all means lack of training which has a result of reduced productivity for investments that sometimes cost millions of pounds. The third and fourth approach of the subject can be associated with these data in order to understand them spherically.

Frequency of virus attacks on businesses, 2005

United Kingdom

Percentages



Frequency of virus attacks on businesses, 2005

	Once	A few times	Approximately one a month	Approximately one a week	At least one a day
Virus infection	32	56	7	1	4
Denial of service	53	35	4	4	4

Graph – Table 3: Frequency of virus attacks on businesses.

One of the most interesting graphs from our data set is shown above. In 2005 32% of UK's businesses had at least once a virus infection and 53% of them have been denied to serve their customers electronically. Numbers are always remorseless. One out of two businesses had its systems disabled even for a while and because of that lost money, prestige, reputation and of course clients some of them devoted. Marketing-speaking the effort to recapture a satisfied and devoted customer, that for some reason lost his trust to a business is many times more than to win him for the first time. Every time that a website is down, especially an e-commerce site, clients and money are lost and this has to do both with technology and policy for how to use it properly and beneficiary. All of the approaches referenced in our theoretical foundation can be combined with these data, especially the second one because nowadays outsourcing has a major role in servicing many businesses electronically and remotely.

Estimated total cost of computer-enabled crime, by type of crime, 2004

United Kingdom		£ million
	Firms with 100 to 1,000 employees	Firms with over 1,000 employees
Viruses, worms or trojans	70,8	676,7
Financial fraud	68,2	622,3
Denial of service	2,9	555,2
Equipment theft	28,8	383,7
Telecoms fraud	0,1	77,7
Systems used for criminal/illegitimate purposes	0,2	46,1
Unauthorised access to business system	2,2	43,7
Theft of information/data	3,3	33,3
Sabotage of data or networks	0,7	5,7
Website defacement	0,1	-

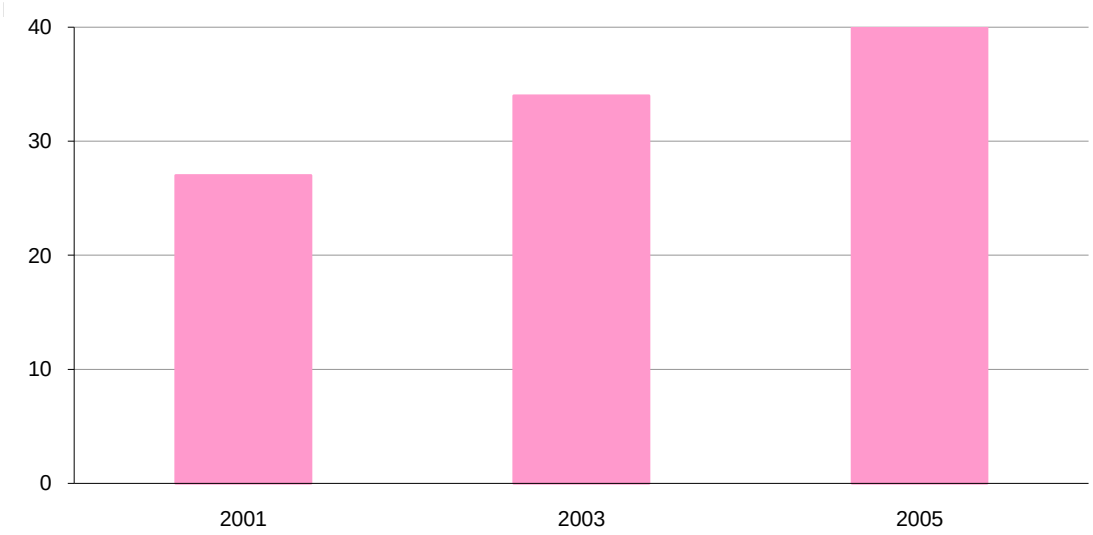
Table 4: Cost from computer-enabled crime in United Kingdom during 2004

From the board above we can realize two different situations concerning information security and its economic consequences. If we sum the amounts of computer-enabled crime cost for the firms with over 1,000 employees, we find out it is about 2.5 billion pounds in only one year, just during 2004. Also interpreting the figures we realize, in both business categories, that the biggest percentage of the cost comes from the first four categories. Examining more the data it is obvious that with better policies and technology much of the cost could have been avoided. Denial of service attacks and viruses infections can be reduced when an firm adopts a certain security policy, invests in technology and trains its security and IT professionals in order to fulfill the expectations of the management by cutting costs from computer-enabled crime. All our theoretical approaches can be used to combine them with the data, giving some extra notice to our third approach about confidentiality and availability.

.

Businesses with a formal information security policy

United Kingdom



Businesses with a formal information security policy

United Kingdom	Percentages
2001	27
2003	34
2005	40

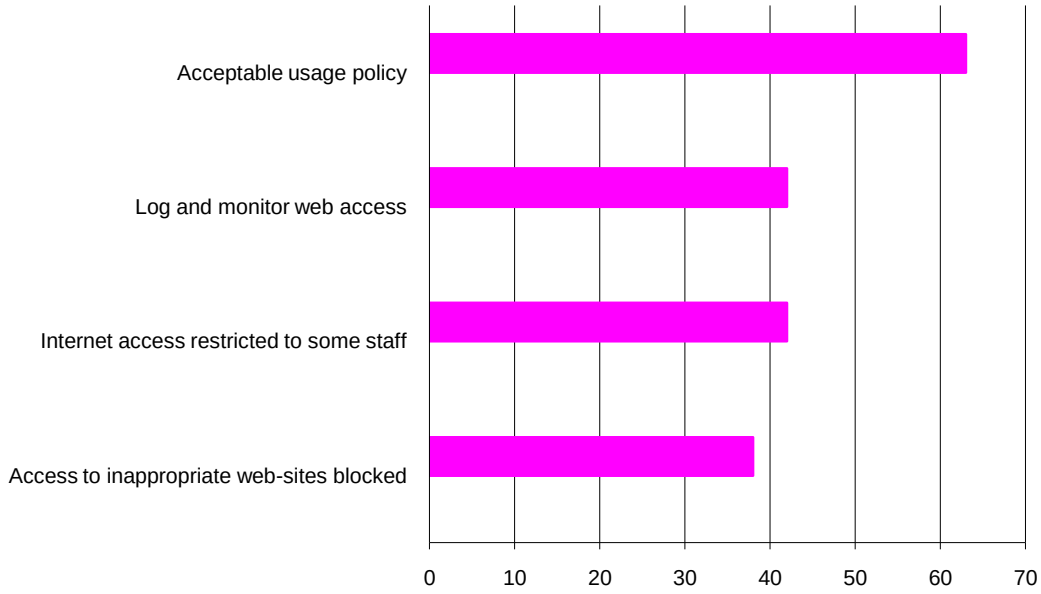
Graph – Table 5: Businesses in the United Kingdom with a formal security policy

The data set shown above gives us an interesting information. During the last decade there was a continuing increase in the percentage of businesses with a formal security policy. We have just showed the cost from computer-enabled crime in the UK which is directly connected with security policy as we mentioned. If the increase continues we should expect the cost from such incidents to degrade. Again all our theoretical approaches can be used to interpret the data because all of them are dealing with security policies.

How businesses control staff Internet usage, 2005

United Kingdom

Percentages



United Kingdom	Percentages
Access to inappropriate web-sites blocked	**38**
Internet access restricted to some staff	**42**
Log and monitor web access	**42**
Acceptable usage policy	**63**

Graph-Table 6: How Businesses in the UK control staff Internet usage during 2005

The data shown above show us a more specific view on the subject of security policy. IT administrators with security experts are using certain techniques to deal with staff internet usage. Inappropriate usage can be catastrophic for a business because of the cost it involves. In order to maximize the effects of such policies, all types of techniques should be used, like the four mentioned in the board. Only then we can expect that the efforts of the IT department matched with the efforts of all personnel can be profitable for the business by means of less cost from inappropriate usage. We should always remember that a business does not makes profit only by selling goods or services, but also by cutting costs from its everyday operation, especially costs that can be reduced only by using the existent infrastructure and personnel more effectively. The reader may find our third approach very useful in order to understand the meaning of controlling and securing internet usage in a business.

We tried through the statistics to show a more quantitative view on the subject, because most of the times numbers do not lie. The numbers show that along with the boost of IT usage in the enterprises, policies about that usage have to be adopted in order to optimize it. Expenditure for IT is rising and will continue rising in the future and that is why enterprises should become more professional about it.

CONCLUSION

The subject connects two different sciences, information technology and that of economics. Combined, the two sciences can answer more questions than each of them alone. One can present information security only from the side of technology, by means of hardware and software but almost everything in life has a cost. That is why we have to give an economic perspective of the subject. We tried to present four different approaches in information security economics, in order to give a multilateral view with the help of statistical data, but we give a closer view into the last one, that of outsourcing by analizing the work of several researchers on the subject.

We recall the continuous battle between IT experts and administration in businesses, because administration always want to cut costs and IT staff always want to be up to date in terms of security within their budget. The battle continues because IT experts have to defend their budgets from people that understand mostly economic terms, so they have to convince them using their language. Using the word ‘’cost’’ always works because the consequences of investing less money than needed for information security, usually leads to cost a lot more than the investment itself or the data that a business want to protect.

Our statistical data designate the volume of electronic crime, malicious breaches in data centers, credit card frauds e.t.c. nowadays and the economic costs of them both in businesses and their clients. Having in our minds the usage of computers in our everyday life, we can assume the importance of information security especially in e-commerce. During the last decade there was a boost in that field and a whole new economy emerged, so by understanding and investing in information security this field is going to bloom furthermore and create new jobs and wealth.

Businesses only recently started to certify themselves in information security by applying certain policies and behaviours in the use of data within their infrastructure. Job positions for IT security experts only recently have been created and such professionals will be valuable and very well paid in the near future. Firms without a formal information security policy will fall behind and lose face and profit from its competitors, because first of all the security of the firms’ data and also its clients will not be at the highest level available. Without a security policy, there will not be proper training for the staff and there will not be proper usage of the investments for information security. The ideal sum of investment usually comes from the ideal usage of it and not from the volume of it and from its side the ideal usage comes from ideal policies. That is why we mention the example from US Banks with smaller budgets having better results in information security than European ones, because of differences in thinking within their security philosophy.

What we have to keep in our minds is that information security is a play with many actors, acting within a business or not. Only by cooperation they can reach the highest level of security. Administration, IT department and third partners should be aware of their roles and be able to cooperate, synchronize and find common ground in order to reach their common target, to provide security for informations and inspire trust to the market, to the clients which sometimes is even better.

Especially about the third partners, the enterprises that outsource their facilities, experience and staff in the field of IT, we can summarize some interesting findings. There is a tremendous increase into that field that is going to continue furthermore in the near future. It is a unique way to have an IT department but without having a single person as IT staff in your business. One can just apply to one of the many companies to give him his 'own' IT department and services only by giving a monthly fee. But the truth is it's not that simple. The right selection of the third partner is the most important processes when the time comes to outsource IT in an enterprise. The right selection of which part of the IT department is going to be outsourced is also really serious. And all that for what price, because in terms of economics everything has a price?

Nowadays IT is one of the most important departments in an enterprise, because almost everything depends its everyday function more or less in Information Technology applied in each field of an enterprise. Outsourcing one of the most important departments in an enterprise should always be a high administrative level decision but from an IT-wise administration.

Of course the essay has limitations which we have to refer. Dealing with such a new and unique subject that produces new knowledge every day makes a research always fall behind, because in a subject of only 10 years history a six month period of time is huge. That is a problem when you deal with subjects that are in progress.

Also it is difficult to find statistical data from various sources because it is a really new subject. Finding data for security measures is really hard because most times such data are kept within the enterprises for internal use. The data found from the UK's Office for National Statistics are unique because they summarize knowledge on the subject but it has its limitations also because its data is only up to 2006.

Approaching holistically the subject gave us the help to understand it, as we mention researchers with different experiences, knowledges and interests and we give a step to continue the research furthermore in the future.

REFERENCES

[1]. (L. JEAN CAMP, *The State of Economics of Information Security*, available at: http://www.is-journal.org/V02I02/2ISJLP189-Camp.pdf, p:1,2).

[2]. (Ta-Wei Wang, *Essays on information security from an economic perspective*, Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, CERIAS Tech Report 2009-24, 2009, p: 11,13,14,17-19,20-24,42,43,48-52,109,110, available at: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-24.pdf).

[3]. (Zach Z. Zhou, M. Eric Johnson, *The Impact of Information Security Ratings on Vendor Competition*, Center for Digital Strategies The Tuck School of Business Dartmouth College , 2009, p: 2,3,4,23,24, available at: http://weis09.infosecon.net/files/134/paper134.pdf).

[4]. (Christos Ioannidis et al, *Investments and Trade-offs in the Economics of Information Security***,** School of Management, University of Bath, Hewlett-Packard Laboratories Bristol UK, University of Aberdeen Business School Aberdeen, 2009, p: 1,2, available at: https://commerce.metapress.com/content/v8q694550u26xwq5/resource-secured/?target=fulltext.pdf&sid=gk5kqx55ifckqb45lb2l4k45&sh=www.springerlink.com).

[5]. (Ross Anderson, *Why Information Security is Hard An Economic Perspective*, University of Cambridge Computer Laboratory, 2001, p: 1,2, available at: http://www.acsac.org/2001/papers/110.pdf).

[6]. (National Statistics Online, Focus on the Digital Age – 2007 – Data and Full Report, available at: http://www.statistics.gov.uk/STATBASE/Product.asp?vlnk=14797)

[7]. (Sandoval, G., and Wolverton, T. 2000. *Leading web sites under attack*. Retrieved April 17, 2007, from http://news.com.com/Leading+Web+sites+under+attack/2100-1017_3-236683.html).

[8]. (CSI/FBI. 2008. The CSI/FBI computer crime and security report in 2007, Retrieved May 29 2009, from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf).

[9].(Lohmeyer, D. F., McCroy, J., and Pogreb, S. 2002. "Managing information security," *The McKinsey Quarterly*, Retrieved May 29 2009, from http://news.cnet.com/Managing-information-security/2009-1017_3-933185.html).

[10]. (Jorgensen, B. N., and Kirschenheiter M. T. 2003. "Discretionary risk disclosures," *The Accounting Review* (78:2), pp. 449-469).

[11]. (Skinner, D. J. 1994. "Why firms voluntarily disclose bad news," *Journal of Accounting Research* (32:1), pp. 38-60).

[12]. (Sohail, T. 2006. *To tell or not to tell: market value of voluntary disclosures of information security activities*. Unpublished doctoral dissertation, University of Maryland, Maryland).

[13]. (DiRomualdo, A., and V. Gurbaxani. 1998. "Strategic Intent for IT Outsourcing", Sloan Management Review, 39(4), 67-80).

*[14]. (*Macura, I. and E. Johnson. 2009. "Information Risk and the Evolution of the Security Rating Industry," Working Paper, Tuck School of Business at Dartmouth College. http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoRR7.pdf

[15]. (Stoneburner, G., A. Goguen, and A. Feringa. 2002. “Risk Management Guide for Information
Technology Systems”, National Institute Standards and Technology (NIST) Special Publication 800-30).

[16]. (Kark, K. 2008. “Can Moody’s Solve Your Third Party Assessment Problem?” http://blogs.forrester.com/srm/2008/05/can-moodys-solv.html).

[17]. (Kliger, D., and O. Sarig. 2000. “The Information Value of Bond Ratings”, The Journal of Finance, 55(6), 2879-2902).

[18]. (Shapiro, C. 1986. “Investment, Moral Hazard, and Occupational Licensing”, The Review of Economic Studies, 53(5), 843-862).

[19]. *(*Anderson, R., B¨ohme, R., Clayton, R., Moore, T.: Security economics and the internal market. Report to the European Network and Information Security Agency, ENISA (2007), http://www.enisa.europa.eu/doc/pdf/report sec econ & int mark 20080131.pdf)

[20]. *(*Gordon, L.A., Loeb, M.P.: The Economics of Information Security Investment. ACM Transactions on Information and Systems Security 5(4), 438–457 (2002))

[21]. *(*Hausken, K.: Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information Systems Frontiers 8(5), 338–349 (2006))

[22]. (Willemson, J.: On the Gordon & Loeb Model for Information Security Investment. In: Proc. WEIS (2006), http://weis2006.econinfosec.org/docs/12.pdf)

[23]. (RJ Anderson, \Why Cryptosystems Fail" in *Communications of the ACM* vol 37 no 11 (November 1994) pp 32{40)

[24]. (CERT, Results of the Distributed-Systems Intruder Tools Workshop, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org/reports/dsit_workshop-final.html, December 7, 1999)

[25]. (H Varian, `*Intermediate Microeconomics { A Modern Approach'*, Fifth edition, WW Norton and Company, New York, 1999; ISBN 0-393-97930-0)

[26]. (Matilda Alexandrova, *INTERNATIONAL OUTSOURCING: INCENTIVES, BENEFITS AND RISKS FOR THE COMPANIES IN SEE COUNTRIES,* Department of Management University of National and World Economy, Sofia, p: 2-3, available at: http://www.asecu.gr/files/RomaniaProceedings/02.pdf)

[27]. (NOOR HABIBAH ARSHAD, YAP MAY-LIN, AZLINAH MOHAMED, *ICT Outsourcing: Inherent Risks, Issues and Challenges,* Faculty of Information Technology & Quantitative Sciences Universiti Teknologi MARA, MALAYSIA, p:2-8, available at: http://www.wseas.us/e-library/transactions/economics/2007/24-107.pdf)

[28]. (John S. Bojonny, *IT Outsourcing*, Montgomery College, EDUCAUSE Evolving Technologies Committee, p: 1-4, available at: http://net.educause.edu/ir/library/pdf/DEC0505.pdf).

[29]. (David C. Chou , Amy Y. Chou , SOFTWARE AS A SERVICE (SaaS) AS AN OUTSOURCING MODEL: AN ECONOMIC ANALYSIS , Dept. of CIS, Eastern Michigan University, Ypsilanti, School of Information Technology, Illinois State University, Normal, p:2-6, available at:

http://www.swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S469.pdf).

[30]. (Jerry E. Durant, The NEW Economics of Global Outsourcing, Chairman Emeritus in The International Institute for Outsource Management, January 2009, p: 6, available at: http://www.outsourcing.com/pdf_files/04.10.2009/The%20NEW%20Economics%20of%20Outsourcing.pdf).

[31]. (Ursula Huws et al, *Status Report on Outsourcing of ICT and Related Services in the EU***,** Analytica and Forschungs- und Beratungsstelle Arbeitswelt, p: 5, available at : http://www.uniglobalunion.org/unisite/sectors/ibits/moos/pdfdocs/R4.pdf).

[32]. (Brent R. Rowe, Will Outsourcing IT Security Lead to a Higher Social Level of Security?, RTI International , p: 2-3, 5-6, 8, 11-13, available at: http://weis2007.econinfosec.org/papers/47.pdf).