Analyzing the Economic Impacts of Security Breaches Due to Outsourcing

Dimitrios Koumaridis, Emmanouil Stiakakis, and Christos K. Georgiadis

University of Macedonia, Department of Applied Informatics,
Egnatia 156, 54006 Thessaloniki, Greece
{koumaridis,stiakakis,geor}@uom.gr

Abstract. In our study, we present four different approaches on the subject that are connected more or less to each other, giving more attention on outsourcing security issues. A case study for the use of outsourced services is also presented using empirical data from an insurance company. This work concludes with an overview of our research, its limitations and by giving some research questions for future work.

Keywords: security economics, outsourcing, security breach.

1 Introduction

The aim of this work is to identify and examine some of the major approaches in the area of security economics. More specifically, four different approaches are examined. We start by presenting them in the section of theoretical background and then we mostly emphasize on the one dealing with the outsourcing policy of companies. These four approaches are connected to each other since they deal with the same subject but from a different point of view.

The first approach is a research by Wang [1] about the effects that disclosures have in business economics, regarding security policies and cases of security breakdowns. The second approach by Ioannidis et al. [2] presents the "conflict" between system administrators and system users about confidentiality and availability. The authors also present the endless effort of the administrators to exploit their budgets properly in order to raise their effectiveness. The third approach on the subject of security economics comes from Anderson [3] and is more behavioral rather than technical, as security is a combination of technology and policy over the proper usage of it. It deals mainly with differences in sentiments upon information security. The fourth approach deals with the rising development of the third partner services in many businesses and the problems occurring from the adoption of this outsourcing policy. It is of great importance that a company gives the opportunity to another company to process crucial and sometimes top secret data. The last approach is the main topic of our work. We conclude with a case study concerning a Greek insurance company about the usage of outsourced services and their impacts.

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 156–163, 2012.

2 Theoretical Background – Literature Review

For a non-experienced observer, the aforementioned approaches are not connected to each other; however, there are certain similarities among them. These similarities will be understood once the following presentation of the approaches has been completed.

2.1 The Effects of Information Disclosures in Business Economics

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 [1]. In order to address the issues and better manage information security risks, researchers and managers have strived to better understand and assess information security risks.

Some firms announce risks related to information security publicly. There are two competing motivations from the literature why firms disclose risk factors. On the one hand, the disclosure of risk factors may contribute to the reduction of the uncertainty that investors have regarding the firm's performance [4]. On the other hand, a firm may disclose risk factors in order to reduce its future litigation costs associated with adverse events [5]. In the information security context, any 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.

Wang [1], through his research, tries to further examine 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 non-disclosing 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. General market participants can actually 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. There is a strong 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. By taking advantage of the different perceptions among investors, it is shown that, on average, one can make about 300% annual profit around the breach announcement date.

2.2 Cost vs. Performance

In our second research approach, we focus on the relation between cost and performance [2]. Information security and network integrity are issues of the utmost importance to both users and managers [6]. 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 an acceptable operational state.

Gordon and Loeb in [7] adopt an optimizing framework for the economics of information security, which provides 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, they 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 [8-9] 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 authors give examples where optimal investment ranges between 50% and 100% of the value of information that is protected.

2.3 The Human Factor

The third approach is more theoretical, with a subject that deeply has to do with the human factor and more specifically the human attitude. Anderson [3], one of the pioneers in the field, deals with information security putting forward a contrary view rather 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 about the human factor and mainly the human behavior is given in [10], concerning fraud against auto teller 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, and this gave US banks a motive to protect their systems properly. But in Great Britain, Norway, and the Netherlands, the burden of proof lies on the customer: the bank is 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.

2.4 Outsourcing

Analyzing the last approach (outsourcing), we can understand that it is really tight with the first approach, because the disclosure of such a strategic decision usually affects an enterprise positively or negatively. Positively, because such a decision reduces the fixed costs of the enterprise by giving the effectuation of services somewhere else to a third partner; on the other hand, it 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 secured 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 to the enterprise, because it will possibly stop its usual operation and when something stops functioning usually means losing money. It is even worse to lose reputation in the market since the enterprise has to fight hard to regain it. A disclosure of such an event will affect 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.

3 Analyzing Outsourcing-Related Security Issues

Zhou and Johnson [11] are among the researchers that work on the problem of security breaches due to 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.

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 [12]. Many widely publicized

security breaches have been the consequences 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 offerings 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.

There have been recently 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 sides (rather than each firm individually assessing each of their vendors) [13]. 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 [14]. 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.

Zhou and Johnson, through their research, have tried to answer some demanding questions, as for example, if risk ratings always benefit the high-security service provider (or hurt the low-security service provider). If not, how does the risk rating affect different service providers under different market conditions? Another of their concerns is whether risk ratings always benefit the most demanding customers who desire highly secured business partners? And lastly, does risk rating increase social welfare? Some very interesting results have been found: 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 low-security 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. Since ratings clearly reveal the security of providers, such information helps service providers to differentiate themselves, and thus can benefit both.

While the literature [15] shows that improved information always benefits the high-type customer, the model 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 high-security 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 ratings should be encouraged by social planners.

4 A Case Study of an Insurance Company

It is always useful to present data from the daily operation of a company. We present the case study of the company Infotrust SA. This is an insurance brokerage company located in Thessaloniki, Greece, with two other branches in Athens and Rhodes. Its functions are between the functions of insurance advisors and those of insurance companies. However, there is the need for this company 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 to another company using Software as a Service.

A personal interview was conducted with the company's IT administrator. The questions used in this interview and the answers given (as "yes" or "no" to the answer, for brevity's sake) are presented in Table 1.

Table 1. Questions used in the personal interview with Infotrust'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) Are there any hidden costs?		✔
8) Is there any unclear cost to benefit relationship?		✔
9) Are the data secured? (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 is 40, so forty licenses (e-mails) are needed, at least. Each license 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 a number of employees and much equipment, it is better, of course, to outsource those services.

One major issue for this 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 states 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.

5 Discussion

As we noticed there are connections between the four different approaches because information security encompasses technology, economics, and human behavior; hence, it is not an one-dimensional topic. It can be viewed from many aspects. That is why problems about information security are not unilateral and can be solved only through cooperation of people in all the different fields just mentioned. It would be useful to set some research questions for the readers that could help them continue their own work on the subject.

We have just passed the first decade of activity on this subject and still, especially in developing countries, information security is not a real concern or it is in the hands of IT managers without a real security policy from the administrations. Another question that supplements the first one is whether enterprises are aware of the real dangers that accompany the handling of information, especially in areas when laws about information handling and information security are getting really tough.

Given the continuing increase in IT outsourcing adoption from the enterprises, a final question is whether the related dangers will increase or the enterprises will understand those dangers and take measures to face them.

6 Conclusion

Businesses only recently started to be involved in security economic issues by applying certain policies concerning their data. Firms without a formal information security policy will be less competitive, because security of the business data and also its clients will not be at the highest level available. Without a security policy, there will not be a proper training for the staff and a proper usage of the investments for information security. An ideal investment arises when there is a good usage of it and a good security policy and does not exclusively depend on the volume of it. That is why we mentioned the example of US Banks with smaller budgets having better results in information security than the European ones.

Particularly for the third partners and the enterprises that outsource their activities, some interesting findings can be summarized. There is a tremendous increase in that field that is going to continue furthermore in the near future. It is important to have an IT department but without having a single person as IT staff in this department. The

right selection of the third partner is the most important process when the time comes to outsource IT to an enterprise. The right selection of which part of the IT department is going to be outsourced is also a serious issue. And all that for what price, because in terms of economics, everything in business has a price.

References

1. Wang, T.W.: Essays on Information Security from an Economic Perspective. Center for Education and Research Information Assurance and Security Purdue University. Technical report (2009)
2. Ioannidis, C.: Investments and Trade-offs in the Economics of Information Security. School of Management, University of Bath, Hewlett-Packard Laboratories Bristol UK (2009)
3. Anderson, R.: Why Information Security is Hard: An Economic Perspective. University of Cambridge Computer Laboratory (2001)
4. Jorgensen, B.N., Kirschenheiter, M.T.: Discretionary Risk Disclosures. The Accounting Review 78(2), 449–469 (2003)
5. Skinner, D.J.: Why Firms Voluntarily Disclose Bad News. Journal of Accounting Research 32(1), 38–60 (1994)
6. Anderson, R., Böhme, R., Clayton, R., Moore, T.: Security Economics and the Internal Market. Report to the European Network and Information Security Agency, ENISA (2007)
7. Gordon, L.A., Loeb, M.P.: The Economics of Information Security Investment. ACM Transactions on Information and Systems Security 5(4), 438–457 (2002)
8. 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)
9. Willemson, J.: On the Gordon & Loeb Model for Information Security Investment. In: The Fifth Workshop on the Economics of Information Security WEIS, Cambridge, UK (2006)
10. Anderson, R.J.: Why Cryptosystems Fail. Communications of the ACM 37(11), 32–40 (1994)
11. Zhou, Z.Z., Johnson, M.E.: The Impact of Information Security Ratings on Vendor Competition. Center for Digital Strategies, Tuck School of Business Dartmouth College (2009)
12. Macura, I., Johnson, E.: Information Risk and the Evolution of the Security Rating Industry. Working paper, Tuck School of Business Dartmouth College (2009)
13. Kark, K.: Can Moody's Solve Your Third Party Assessment Problem?, `http://blogs.forrester.com/srm/2008/05/can-moodys-solv.html`
14. Kliger, D., Sarig, O.: The Information Value of Bond Ratings. The Journal of Finance 55(6), 2879–2902 (2000)
15. Shapiro, C.: Investment, Moral Hazard, and Occupational Licensing. The Review of Economic Studies 53(5), 843–862 (1986)