December 2006

Controlling Adverse Selection in Information Security Budgeting: An IT Governance Approach

Yu Wu
University of Central Florida

Controlling Adverse Selection in Information Security Budgeting: An IT Governance Approach

Yu "Andy" Wu
University of Central Florida
ywu@bus.ucf.edu

ABSTRACT

From an agency theory perspective, top management engages the information security function as the agent to manage security for the organization. Adverse selection in InfoSec budgeting occurs when top management cannot validate the soundness of the ISF's requests for InfoSec investments. IT governance may control adverse selection because it aims at the alignment between business and IT and facilitates monitoring and bonding. Three types of governance mechanisms – process-based, structural, and relational, are analyzed. They are hypothesized to help to reduce information asymmetry. Less asymmetry leads to reduction in adverse selection, which, in turn, boosts top management confidence in InfoSec success. Based on these, a research model is presented and survey research designed to test it.

Keywords

Information security, agency theory, adverse selection, information asymmetry, IT budget.

INTRODUCTION

Organizations' investments in information security (InfoSec) are becoming sizable. The 2005 CIO/PWC (2005) InfoSec survey shows that, on average, 13% of an organization's IT budget goes to InfoSec. It is important for an organization to ensure that it does not under- or over-invest in InfoSec. An organization's information security function (ISF) is increasingly required to justify their budget in financial terms (Gordon, Loeb, Lucyshyn, and Richardson, 2005), such as return on investment (ROI). The ISF thus should properly relate InfoSec spending requests to business security requirements (Schweitzer, 1996). The ISF's success, or lack thereof, in doing this, however, can be difficult for the top management to verify, because of an information asymmetry between them. From an agency perspective, an adverse selection problem presents in this respect.

Controlling adverse selection in InfoSec budgeting can be particularly difficult, because the information asymmetry is exacerbated by intangibility of InfoSec outcomes. It is very difficult, if at all possible, to calculate expected financial returns from InfoSec investments (Newman and Scholtz, 2003; Paquet and Saxe, 2005). Outcome intangibility also undermines outcome-based contracts, which traditional agency literature would prescribe for agency problems in non-programmable tasks such as InfoSec.

To effectively control adverse selection in InfoSec budgeting, therefore, the focus should be on reducing the information asymmetry and improving the alignment between the principal's and the agent's interests. An organizational capability that can be instrumental in this respect is IT governance. Therefore, this study attempts to ask these questions: Does IT governance help top management ascertain that the ISF is requesting the proper security investments? Does IT governance help to reduce the information asymmetry between the ISF and top management and, in turn, adverse selection in InfoSec budgeting? Does IT governance help to increase top management's confidence in InfoSec?

LITERATURE REVIEW

This study draws upon three sources of literature: agency theory, InfoSec, and IT governance.

Agency Theory

Agency relationships exist in virtually all cooperative efforts (Jensen and Meckling, 1976). The *raison d'être* for agency relationships is division of labor. It is comparatively competitive for the principal to engage the agent to perform a task

because the agent possesses more specific knowledge about performing the task (Fama and Jensen, 1983; Jensen and Meckling, 1992). However, the agent's superior information, coupled with the fundamental divergence in interest between the principal and the agent, gives rise to agency problems.

In the agency literature, the agent's superior specific knowledge is usually discussed in terms of the information asymmetry between the agent and the principal. Besides agent's training and expertise, the agent also obtains, in the process of performing the task, private information regarding (a) the actions required for the task, (b) her own actions, and (c) the task's current state. Information asymmetry thus grows between the principal and the agent, with the principal not being able to gain costless access to the agent's private information (Baiman, 1990).

The divergence of interests between the principal and the agent is usually discussed in terms of their differential risk aversion and effort aversion. Since the principal and the agent derive their compensation differently from the task, they form different attitude toward the risks and efforts involved. Agency theorists generally assume that the principal is risk-neutral and the agent is risk-averse (Nilakant and Rao, 1994). Another basic tenet in the agency literature is the agent's innate inclination to avoid expending efforts (Levinthal, 1988).

Given the information asymmetry and differential risk/effort aversion, the agent may or may not behave in the best interest of the principal (Eisenhardt, 1989). Researchers generally agree on two types of agency problems – moral hazard and adverse selection. Moral hazard refers to the agent exercising less than enough effort (Mills, 1990). Adverse selection is the principal's inability to determine whether the agent is using her private information to make the right decisions and/or exert the appropriate types of effort that best serve the principal's interest (Adams, 1994; Arrow, 1985; Clark, 1993; Mills, 1990; Nilakant and Rao, 1994).

Adverse Selection In Infosec Budgeting

Both differential risk aversion and information asymmetry clearly are at play in InfoSec budgeting. The ISF staff tends to be naturally risk averse while top managers often thrive on taking risks (Berinato, 2002; Ernst & Young, 2004; Kairab, 2005; Schweitzer, 1987). What the ISF believes to be of paramount importance may not be seen by top management as critical to the business (Schweitzer, 1996), because differential risk aversion can lead the agent to choose different courses of action than what the principal would prefer (Eisenhardt, 1989).

Information asymmetry in InfoSec can be pronounced. InfoSec technical competence demands a significant depth of technical knowledge (Schweitzer, 1987), which is costly to transfer from the agent to the principal. Most characteristically, in InfoSec the asymmetry is exacerbated by the large degree of intangibility of outcomes. InfoSec is a function where when everything goes well, nothing happens (PriceWaterhouseCoopers and *CIO* Magazine, 2004). When InfoSec measures work as intended, the apparent absence of damage to information may be considered as evidence that no threat exists (Kairab, 2005; Paquet and Saxe, 2005; Schweitzer, 1996). This creates a unique challenge for top management to verify the quality of the ISF's request for InfoSec investments, hence the adverse selection problem.

Control Of Agency Problems

Agency researchers have long focused on the employment contract or structure of compensation as the major means to control agency problems (Nilakant and Rao, 1994). A dichotomy of controls is often proposed. If the behaviors required for task performance can be predefined and readily observed, they can be used as the basis for rewarding the agent. If the outcomes from the task is easily measured, the reward may be based on the outcome (Eisenhardt, 1985, 1989; Nilakant and Rao, 1994). However, neither provides adequate solution to agency problems in InfoSec because InfoSec tasks are usually non-programmable and many of InfoSec outcomes are intangible. Moreover, an *ex ante* contract is never sufficient and more sophisticated governance is required (Baiman, 1982, 1990; Spraakman, 1997).

Monitoring is an important governance method that receives much attention in the managerial accounting literature. It refers to the activities undertaken by the principal to reduce the loss of utility caused by adverse selection or moral hazard (Adams, 1994; Jensen and Meckling, 1976; Mills, 1990). Information asymmetry can be reduced because the principal is able to tap the agent's private information through monitoring (Adams, 1994; Baiman, 1990; Kalbers and Fogarty, 1998).

However, there is a limit to what monitoring can provide (Jacobides and Croson, 2001). Besides monitoring, the agent may be motivated to bond to the principal (Nilakant and Rao, 1994). Bonding refers to the activities undertaken by the agent to assure the principal of some minimum level of performance (Adams, 1994; Jensen and Meckling, 1976; Mills, 1990). Bonding activities typically involve obtaining credentials such as CPA and MD, developing goodwill, and offering guarantees (Mills, 1990).

Eisenhardt (1985) suggests that when neither behavior- nor outcome-based controls is effective, control through reduction of divergence of preferences is appropriate. IT governance, with its primary goal being the alignment of IT and business objectives, can be effective in controlling agency problems in InfoSec.

IT Governance

IT governance is an organizational capacity through which the board and top management guide the direction of IT toward better alignment with business (Van Grembergen, De Haes, and Guldentops, 2004). Three types of governance mechanisms can be implemented to that end.

Process-based mechanisms are IT management techniques to ensure that daily behaviors are consistent with IT policies and that all stakeholders are involved in the effective management and use of IT (Weill and Ross, 2004). They often appear as the institution of standard procedures embedded in formalized decision-making methodologies and management frameworks, e.g., IT Governance Institute's (2000) Control Objectives for Information and Related Technology (CobiT), balanced scorecards, service level agreements, etc. (Peterson, 2004; Weill and Ross, 2004).

Structural mechanisms are organizational units and roles created to properly locate decision-making responsibilities and to promote horizontal connection between IT and business functions (Peterson, 2004; Peterson, O'Callaghan, and Ribbers, 2000; Weill and Ross, 2004). Examples include formal groups such as executive teams, committees, councils, task forces, and other integration structures (Peterson, 2004; Peterson et al, 2000; Weill and Ross, 2004).

Relational mechanisms are the organizational practices aimed at encouraging voluntary two-way communication, mutual understanding, and collaboration between business and IT (Peterson, 2004; Van Grembergen et al, 2004). Examples include direct (informal) contacts, lobbying, joint performance incentives and rewards, collocation of business and IT managers, cross-functional training, job rotations, continuous education, etc.

RESEARCH MODEL AND HYPOTHESES

The three types of IT governance mechanisms hold the potential for an organization to reduce the information asymmetry and divergent interests between top management and the ISF.

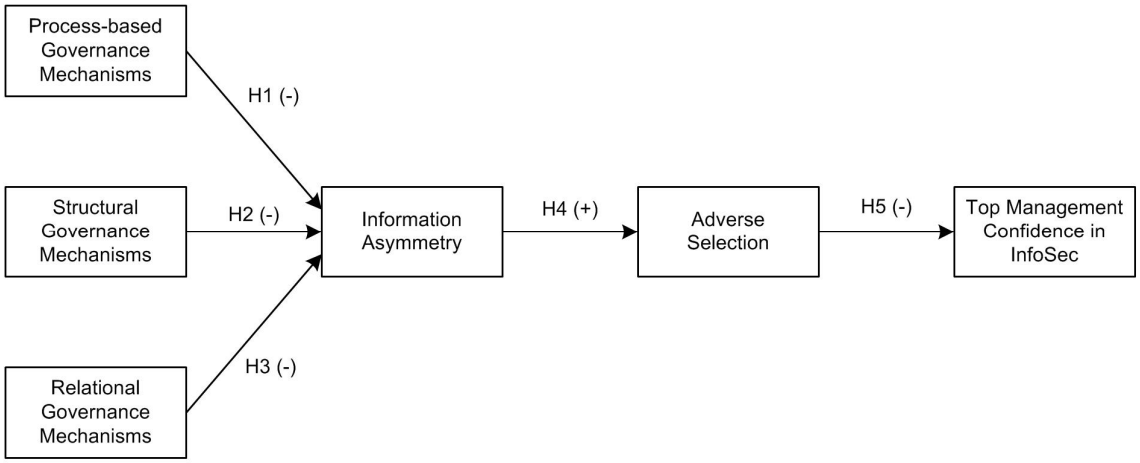

Figure 1. Research Model

An important function of process-based mechanisms is to institute monitoring in the IT processes, including InfoSec. Monitoring allows top management better access to the agent's private information. Therefore,

H1: Process governance mechanisms reduce the information asymmetry between the ISF and top management.

Structural mechanisms ensure proper composition and positioning of the organization's monitoring function, such as internal auditors. As the result, the monitoring information gathered is more likely to be complete, impartial, and accurate. Therefore,

H2: Structural governance mechanisms reduce the information asymmetry between the ISF and top management.

Relational governance mechanisms encourage the ISF to initiate frequent communication with top management regarding their capabilities and business savvy, the organization's current InfoSec status, new InfoSec threats and defense measures, etc. Therefore,

H3: Relational governance mechanisms reduce the information asymmetry between the ISF and top management.

When the information asymmetry between the ISF and top management is reduced, the latter will perceive themselves as more informed about ISF staff's background and their technical capabilities, their reasoning in choosing courses of action, their sincerity in participating constructively in the cooperative efforts of InfoSec, and the current state of the organization's InfoSec. Therefore,

H4: Reduction in information asymmetry between the ISF and top management leads to lower adverse selection in ISF's InfoSec budget requests.

The ultimate goal of reducing agency problems in InfoSec budgeting is to achieve an effective InfoSec program. If top management perceives lower adverse selection in InfoSec budgeting, it will have more confidence in InfoSec investments meeting the organization's security requirements properly, hence more confidence in its InfoSec program. Therefore,

H5: Lower adverse selection in the ISF's InfoSec budget requests leads to higher top management confidence in InfoSec success.

METHODOLOGY

This study will be implemented as survey research. The unit of analysis will be the organization. The intended respondents will be members of top management (CEO, CFO, or COO) in the organization. Data collected from the survey will be analyzed using structural equation modeling (SEM) tools.

Instrument Development

There are no existing instruments for constructs in this study. Moreover, all constructs represent latent variables (factors) that should be measured with directly observable variables (indicators). Therefore, the researcher will create a new instrument with items to measure the indicators.

Validation of newly created instruments is an often neglected however essential requirement for quantitative research in IS (Boudreau, Gefen, and Straub, 2001; Straub, 1989). Following Straub, Boudreau, and Gefen (2004), a set of validation tests will be conducted to validate the instrument's psychometric properties. The researcher is assembling a domain expert panel for the development, validation, and testing of the instrument.

An initial item pool will be generated based on review of extant literature and discussion with InfoSec practitioners. Afterwards, pretest will be performed on the items via interviews with the expert panel and conceptual methods such as Q-sorts (Kerlinger, 1973). Similar to Straub (1989), this pretest will be a largely qualitative evaluation performed on the items' content validity, construct validity, and reliability.

After the instrument is revised, a pilot test will be performed. Using procedures that will be used in the final administration of the survey, the complete instrument will be administered to a small number of respondents who are representative of the population (Bourque and Fielder, 2003).

Survey Administration

Once the survey instrument is finalized based on pilot test results, it will be distributed to the sample of the survey. To select organizations for the sample, commercial databases/directories of organizations will be used. Cluster sampling (Fink, 2003) will be done. To reach a larger sample and to boost response rate, the researcher is seeking organizational sponsorship from InfoSec organizations such as the Information Systems Audit and Control Association (ISACA).

Since SEM techniques will be the primary analytical tool, the sample size should be such that there is sufficient power to detect the intended effects (Sivo, Saunders, Chang, and Jiang, 2006). For covariance-based methods such as AMOS and LISREL, the minimum size of the sample should be at least five respondents per indicator in the model (Schumacker and

Lomax, 2004). For partial least squares (PLS), it is at least ten times the number of indictors for the most complex construct (Gefen, Straub, and Boudreau, 2000).

A traditional mail survey questionnaire will be administered. However, the questionnaire also is available online and the respondents may choose to fill out the printed or the online version, but not both.

Data Analysis

After data is collected from the survey, first, descriptive statistics will be run on the early and late responses to check whether the two groups differ in any systematic ways, such as respondent demographics. All responses will also be analyzed for difference across organization size, industry, and geographic location.

Afterwards, the research's measurement model will be validated. Statistical tests will be performed on the data to validate the instrument's construct validity and reliability, which includes internal consistency and unidimensionality (Straub et al, 2004).

Once the measurement model is validated, further SEM analyses will be performed to examine the structural model. The likely tool that will be used is AMOS or LISREL. However, since response to InfoSec research survey can be extremely low (Kotulic and Clark, 2003), if the number of responses prohibits the use of covariance-based SEM tools, PLS will be used instead.

CONCLUSION

Adverse selection in InfoSec budgeting occurs when top management cannot effectively validate the soundness of the ISF's requests for InfoSec investments. This is due to the information asymmetry and differential risk aversion between them. In InfoSec, the asymmetry can be acute because InfoSec outcomes often are intangible.

Good IT governance may effectively control adverse selection. Three categories of mechanisms of IT governance – process-based, structural, and relational, are analyzed. It is hypothesized that these mechanisms contribute to the reduction of information asymmetry. Less asymmetry leads to reduction in adverse selection, which, in turn, increases top management confidence in InfoSec success. Based on these, a research model is presented and survey research designed to test it. A new survey instrument will be created and validated to measure the constructs in the model. Plans on survey administration and data analyses methods are presented.

REFERENCES

1. Adams, M. B. (1994) Agency theory and the internal audit, *Managerial Auditing Journal*, 9, 8, 8-12.
2. Arrow, K. J. (1985) The economics of agency, in J. W. Pratt & R. J. Zeckhauser (Eds.), Principals and Agents: The Structure of Business (pp. 37-51), Harvard Business School Press, Boston, MA.
3. Baiman, S. (1982) Agency research in managerial accounting: A survey, *Journal of Accounting Literature*, 1, 154-213.
4. Baiman, S. (1990) Agency research in managerial accounting: A second look, *Accounting, Organizations and Society*, 15, 4, 341-371.
5. Berinato, S. (2002) Finally, a real return on security spending. *CIO Magazine*, February 15, 2002, Retrieved May 15, 2006, from <http://www.cio.com/archive/021502/security.html>.
6. Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001) Validation in information systems research: A state-of-the-art assessment, *MIS Quarterly*, 25, 1, 1-16.
7. Bourque, L. B., & Fielder, E. P. (2003) How to Conduct Self-Administered and Mail Surveys, Sage Publications, Thousand Oaks, CA.
8. Clark, T. (1993) The market provision of management services, information asymmetries and service quality - Some market solutions: An empirical example, *British Journal of Management*, 4, 235-251.
9. Eisenhardt, K. M. (1985) Control: Organizational and economic approaches, *Management Science*, 31, 2, 134-149.
10. Eisenhardt, K. M. (1989) Agency theory: An assessment and review, *Academy of Management Review*, 14, 1, 57-74.
11. Ernst & Young. (2004) Global Information Security Survey 2004, Ernst & Young LLP, Chicago, IL.
12. Fama, E., & Jensen, M. C. (1983) Agency problems and residual claims, *Journal of Law & Economics*, 26, 2, 327-349.
13. Fink, A. (2003) How to Sample in Surveys, Sage Publications, Thousand Oaks.

14. Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000) Structural equation modeling and regression: Guidelines for research practice, *Communications of AIS*, 7, 7, 1-78.
15. Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2005) 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, San Francisco, CA.
16. ITGI. (2000) CobiT 3rd Edition Executive Summary, IT Governance Institute, Rolling Meadows, IL.
17. Jacobides, M. G., & Croson, D. C. (2001) Information policy: Shaping the value of agency relationships, *Academy of Management Review*, 26, 2, 202-223.
18. Jensen, M. C., & Meckling, W. H. (1976) Theory of the firm: Managerial behavior, agency cost and ownership structure, *Journal of Financial Economics*, 3, 305-360.
19. Jensen, M. C., & Meckling, W. H. (1992) Specific and general knowledge, and organizational structure, in L. Werin & H. Wijkander (Eds.), Contract Economics (pp. 251-274), Blackwell Publishers, Oxford, UK.
20. Kairab, S. (2005) A Practical Guide to Security Assessments, Auerbach Publications, Boca Raton, FL.
21. Kalbers, L. P., & Fogarty, T. J. (1998) Organizational and economic explanations of audit committee oversight, *Journal of Managerial Issues*, 10, 2, 129-150.
22. Kerlinger, F. N. (1973) Foundations of Behavioral Research, (2nd ed.) Holt, Rinehart and Winston, New York, NY.
23. Kotulic, A. G., & Clark, J. G. (2003) Why there aren't more information security research studies, *Information & Management*, 41, 597-607.
24. Levinthal, D. (1988) A survey of agency models of organizations, *Journal of Economic Behavior and Organization*, 9, 153-185.
25. Mills, P. K. (1990) On the quality of services in encounters: An agency perspective, *Journal of Business Research*, 20, 31-41.
26. Newman, A., & Scholtz, T. (2003) Can security investments show ROI? *Optimize*, October 2003, 25-28.
27. Nilakant, V., & Rao, H. (1994) Agency theory and uncertainty in organizations: An evaluation, *Organization Studies*, 15, 5, 649-672.
28. Paquet, C., & Saxe, W. (2005) The Business Case for Network Security: Advocacy, Governance, and ROI, Cisco Press, Indianapolis, IN.
29. Peterson, R. R. (2004) Crafting information technology governance, *Information Systems Management*, 21, 4, 7-22.
30. Peterson, R. R., O'Callaghan, R., & Ribbers, P. M. A. (2000) Information technology governance by design, in *Proceedings of the Twenty-first International Conference on Information Systems*, December 10-13, 2000, Brisbane, Australia, 435-452.
31. PriceWaterhouseCoopers, & *CIO* Magazine. (2004) The Global Security Survey 2004.
32. PriceWaterhouseCoopers, & *CIO* Magazine. (2005) The Global State of Information Security 2005.
33. Schumacker, R. E., & Lomax, R. G. (2004) A Beginner's Guide to Structural Equation Modeling, (2nd ed.) Lawrence Erlbaum Associates, Mahwah, NJ.
34. Schweitzer, J. A. (1987) Computers, Business, and Security: The New Role for Security, Butterworth Publishers, Stoneham, MA.
35. Schweitzer, J. A. (1996) Protecting Business Information: A Manager's Guide, Butterworth-Heinemann, Boston, MA.
36. Sivo, S. A., Saunders, C. S., Chang, Q., & Jiang, J. J. (2006) *How low should you go? Low response rates and the validity of inference in IS questionnaire research*, University of Central Florida working paper.
37. Spraakman, G. (1997) Transaction cost economics: A theory for internal audit?, *Managerial Auditing Journal*, 12, 7, 323-330.
38. Straub, D. W. (1989) Validating instruments in MIS research, *MIS Quarterly*, 13, 2, 147-169.
39. Straub, D. W., Boudreau, M.-C., & Gefen, D. (2004) Validation guidelines for IS positivist research, *Communications of the AIS*, 13, 24, 380-427.
40. Van Grembergen, W., De Haes, S., & Guldentops, E. (2004) Structure, process and relational mechanism for IT governance, in W. V. Grembergen (Ed.), Strategies for Information Technology Governance (pp. 1-36), Idea Group Publishing, Hershey, PA.
41. Weill, P., & Ross, J. W. (2004) IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, Boston, MA.