Economic Aspects of Controlling Capital Investments in Cyberspace Security for Critical Infrastructure Assets

By

Dr. Lawrence A. Gordon, Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance, Smith School of Business, University of Maryland

Dr. Martin P. Loeb, Professor of Accounting and Information Assurance, Deloitte & Touche Faculty Fellow, Smith School of Business, University of Maryland

Mr. William Lucyshyn, Research Director, Defense Advanced Research Projects Agency & Senior Research Scholar, School of Public Affairs, University of Maryland

Abstract

A model is developed which demonstrates that control systems for investments in information security have a positive net economic impact on an organization. This positive effect is an increasing function of the degree of asymmetric information (related to moral hazard and adverse selection) between Chief Security Officers and Chief Financial Officers within an organization. The role of externalities is also explored in the context of the model.

I. INTRODUCTION

The nation's critical infrastructure assets include oil and gas production and storage, banking and finance, electrical power and telecommunications, are generally controlled by and dependent on cyber-based information systems and the physical assets to support such systems (Bush, 2001).[1] A key aspect of protecting these infrastructure assets is providing cyberspace security. Indeed, capital investments in cyberspace security have become an issue of growing concern in recent years. One dimension of this concern revolves around the need to view these investments in rationale economic terms, similar to the way that traditional capital investments are considered (e.g., see Gordon and Loeb, 2002, 2003).

The literature on traditional capital investments (often called capital budgeting) is well developed (e.g., see Brealey and Myers, 2000). This literature has focused primarily on the selection phase of such investments (e.g., investments in buildings and equipment) and usually culminates in discounted cash flow (DCF) analyses. The DCF methods most commonly employed are the net present value (NPV) and the internal rate of return

[1] PDD-63 defines Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They are generally privately owned, and function collaboratively and synergistically to provide critical goods and services.

(IRR). More recently, real options concepts have been applied to the selection phase of capital investments (e.g., see Dixit and Pindyck, 1994). During the 1990s, a stream of research has also pointed out the importance of control systems (often called postauditing systems) for traditional capital investments (e.g., see Myers et al., 1991, Neal, 1991; Gordon and Smith, 1992; Gordon et al., 1994). This latter body of research demonstrates that sophisticated control systems for capital investments improves the overall investment strategy and, in turn, the performance of an organization.[2] In other words, properly designed control systems for traditional capital investments have a positive net effect on the performance of organizations. However, one factor that seems to affect this positive relation between firm performance and capital investment control systems is the degree of asymmetric information between central management and lower level management (Gordon and Smith, 1992).

To the extent that cyberspace security investments are similar to traditional capital investments, there is reason to assume that control systems for such investments would provide similar net benefits to those noted above for traditional investments. However, given the unique aspects of capital investments in cyberspace security, the cost-benefit aspects of control systems for such investments are highly uncertain. Unfortunately, there is no existing literature on this issue that can help to resolve this uncertainty. Accordingly, the purpose of the research reported in this paper is to examine the cost-benefit aspects of control systems for cyberspace security investments related to critical infrastructure assets. This examination gives particular attention to the role that asymmetric information and externalities play in assessing the costs and benefits of such control systems.

II. BASIC ARGUMENT

Investments in the Nation's critical infrastructure assets have been of interest to researchers, policy setters and private corporations for decades. For example, in 1982, the U.S. General Accounting Office (GAO) published a report entitled "Effective Planning and Budgeting Practices Can Help Arrest the Nation's Deteriorating Public Infrastructure" (U.S. GAO, 1982). However, the developments with our information-based economy and the accompanying developments with the Internet have substantially changed the focus of this interest. More specifically, in today's world of networked, interdependent computer-based information systems, investments in the security of the Nation's infrastructure assets are as much about cyberspace information systems as they are about physical assets. Evidence attesting to this change is clearly provided in "The Clinton Administration's Policy on Critical Infrastructure Protection" known as Presidential Decision Directive (PDD) 63 (May 1998). That directive defines critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government." PDD 63 established the National Infrastructure Protection Center (NIPC) and the encouraged the creation of the Information Sharing and Analysis Centers (ISACs), among other things. The Critical Infrastructure Assurance Office (CIAO) was also established in 1998 in response to PDD

[2] The term control systems in the capital investments literature refers to the process of monitoring a capital project to verify that investments are meeting its stated objective.

63.[3] "The CIAO's primary areas of focus are to raise issues that cut across industry sectors and ensure a cohesive approach to achieving continuity in delivering critical infrastructure services."

In October 2001, President Bush released Executive Order 13231 entitled "Critical Infrastructure Protection in the Information Age." This Executive Order explicitly noted that "The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted." Those three functions now depend on an interdependent network of critical information infrastructure. Executive Order 13231 established the President's Critical Infrastructure Protection Board and also emphasized the importance of ISACs. This executive order was updated on February 28, 2003 restructuring the National Infrastructure Advisory Council (NIAC), having it report through the Secretary of Homeland Security and giving it oversight responsibilities over the ISACs. The Homeland Security Act of 2002 (H.R. 5005) is the latest and most profound step in emphasizing the importance of the investments in the Nation's critical infrastructure assets, including the information infrastructure. The Homeland Security Act incorporates the CIAO into the Department of Homeland Security under the Information Analysis and Infrastructure Protection Directorate.

Underlying much of the above noted legislation is the concern for cyber-space security. Thus, capital investments in cyberspace security by critical infrastructures operators are a key element of protecting critical infrastructure assets. As with all capital investments, it would seem logical to expect that control systems would improve the effectiveness of cyberspace security investments by: (a) helping to identify corrective measures for particular security projects, (b) providing insight on how to improve future security investment decisions, and (c) providing data to help overcome resistance to proposing and terminating security projects (Gordon, 2000, Chapter 11). Accordingly, to the extent that cyberspace security investments are similar to traditional capital investments, there is reason to assume that control systems for such investments would provide similar net benefits (i.e., the difference between benefits and costs). Furthermore, given the often-cited conflict of interest between Information Security Officers (CIOs) and Chief Financial Officers (CFOs), asymmetric information probably plays an important role in reaping such benefits (as it does with traditional capital investments).

The above notwithstanding, most cyberspace security investments are substantially different than the standard or traditional capital investments. To begin with, these investments are a unique form of cost savings (sometimes called cost avoidance) projects. A key reason they are unique is that observing the potential cost savings is inversely related to the effectives of the investment. In other words, you cannot directly observe the cost savings from prevented (or avoided) security breaches because these breaches never occurred. Another unique aspect of investments in cyberspace security relates to what economists call externalities (or neighborhood effects) due to the connectivity of computer networks. More to the point, the benefits of information

[3] Effective March 1st, 2003 the Critical Infrastructure Assurance Office (CIAO) was officially moved into the new Department of Homeland Security under the Information Analysis and Infrastructure Protection (IAIP) Directorate.

security investments depends on the related security investments of other firms sharing the network (e.g., see Camp and Wolfram, 2000; Varian, 2002).

III. MODEL

The model for analyzing the relation between control systems and the cost savings (i.e., benefits) from investments in information security is based on the argument that as asymmetric information increases the marginal benefits associated with control systems are positive and at least constant, if not increasing. The cost of control systems can also be significant and will also likely be a positive function of the degree of asymmetric information. A part of these costs are fixed, while another part increase with difficulty associated with the design of the control system. However, the marginal cost of such control systems should decrease once an appropriate system is in place. Accordingly, the cost of control systems associated with investments in information security should be increase with increases in asymmetric information, but at a decreasing rate.

In terms of externalities, the model shows that neighborhood effects can shift the relations noted above either upward or downward. In other words, we can have an array of benefit and cost curves associated with the control system for investments in information security.

IV. IMPLICATIONS

The key implications of the model discussed above are three-fold. First, control systems for investments in information security will likely result in a net benefit (i.e., the benefits will likely exceed the costs). Second, the degree to which such improvement will occur is an increasing function of the degree of asymmetric information (related to both moral hazard and adverse selection issues) between the CSO and the CFO. However, this later relation is probably highest in the mid range of asymmetric information. Third, and finally, the relation between asymmetric information and the utilization of control systems for investments in information security are moderated by the impact of externalities.

V. CONCLUDING COMMENTS

Analytically it is shown that control systems for investments in information security can have a positive effect on the cost savings associated with preventing potential security breaches. Of course, in the final analysis, the real effect is an empirical issue. Accordingly, the next step in our research is to target two industries (e.g., telecommunications and transportation) and see how control systems for investments in cyberspace security are employed and to assess the net benefits from such systems. Based on the findings from such an empirical study, it is hoped that the “best practices” associated with control systems for investments in cyberspace security can be identified.

REFERENCES

Brealey, R.A., and S.C. Myers, *Principles of Corporate Finance*, 6th ed. (McGraw-Hill, Inc., N.Y., 2000).

Bush, G. W., “Executive Order 13231 on Critical Infrastructure Protection,” Oct 16, 2001, viewed at http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html

Bush, G. W., “Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security,” Feb 28, 2003, viewed at http://www.whitehouse.gov/news/releases/2003/02/print/20030228-8.html

Camp, L. J., and C. Wolfram, "Pricing Security" , Proceedings of the CERT Information Survivability Workshop, Boston, MA Oct. 24-26, 2000, pp. 31-39.

Clinton, W. J., “Protecting America's Critical Infrastructures,” Presidential Decision Directive-63, May 22, 1998, viewed at http://www.fas.org/irp/offdocs/pdd-63.htm

Dixit, A. and R. Pindyck, Investment Under Uncertainty (Princeton, NJ: Princeton University Press), 1994.

H.R, 5005, “To Establish the Department of Homeland Security, And for Other Purposes,” Nov 25, 2002, became Public Law No: 107-296, viewed at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.5005:

Gordon, L. A., *Managerial Accounting: Concepts and Empirical Evidence* (McGraw-Hill, Inc., N.Y., 5th Ed., 2000).

Gordon, L.A. and M. P. Loeb, “The Economics of Information Security Investments,” *ACM Transactions on Information and System Security*, Vol. 5, No.4 (November 2002), pp. 438-457.

Gordon, L.A. and M.P. Loeb, “Budgeting Process for Information Security Expenditures: Empirical Evidence,” (Working paper, 2003).

Gordon, L. A., M. P., Loeb, and M.D. Myers, “A Note of Postauditing Capital Assets and Firm Performance”, Managerial and Decision Economics (1994), pp. 177-181.

Gordon, L. A. and K. Smith, “Postauditing Capital Expenditures and Firm Performance: The Role of Asymmetric Information, Accounting, Organizations and Society, Vol. 17, No. 8 (1992), pp. 741-757.

Gordon, L. A. and K. Smith, “Postauditing Capital Expenditures and Firm Performance: The Role of Asymmetric Information, Accounting, Organizations and Society, Vol. 17, No. 8 (1992), pp. 741-757.

Myers, M., L. A. Gordon, and N. Hamer, “Postauditing Capital Assets and Firm Performance: An Empirical Investigation,” Managerial and Decision Economics August 1991), pp. 317-327.

Neale, B. “The Benefits Derived from Post-Auditing Investment Projects,” Omega, Vol. 19, Nos. 2/3 (1991).

Varian, H. R., "System Reliability and Free Riding," Proceedings of the First Workshop on Economics and Information Security, University of California, Berkeley, May 2002.