Ungureanu, Mihaela

Article

Information Security as Part of the Overall Corporate Governance – It Governance

CES Working Papers

Provided in Cooperation with:
Centre for European Studies, Alexandru Ioan Cuza University

Suggested Citation: Ungureanu, Mihaela (2013) : Information Security as Part of the Overall Corporate Governance – It Governance, CES Working Papers, ISSN 2067-7693, Alexandru Ioan Cuza University of Iasi, Centre for European Studies, Iasi, Vol. 5, Iss. 2, pp. 300-310

This Version is available at:
https://hdl.handle.net/10419/198250

INFORMATION SECURITY AS PART OF THE OVERALL CORPORATE GOVERNANCE – IT GOVERNANCE*

Mihaela **Ungureanu***

Abstract: *A corporate governance system is not based solely on enforcement actions and incentives in order to obtain performance. In the context of a modern business environment, it must initiate and support research and development, contribute to social stability by harnessing human and cultural capital. Corporate governance plays a key role in improving the efficiency of the capital market through its impact on their operations and financial reporting integrity.*

IT governance has become a necessity due to the increased dependence, which is sometimes critical, against the company's IT resources and due to the IT risks growth and diversification that management must settle, now operating in a heavily computerized environment.

The changes in the informational environment and the expansion of new information technologies in organizations determine more complex and heterogeneous IT infrastructures. An essential issue is represented by the quality and performance of the existing system within an organization.

Keywords: information security; corporate governance; IT governance.
JEL Classification: D82; G34; L86.

INTRODUCTION

The end of the last century was a decisive moment in the evolution and modernization of the corporate governance concept, as a part of scientific management. Several studies have highlighted the importance of such a system that works well grounded in optimal conditions, according to some set parameters, aiming to minimize conflicts, increasing efficiency, and encouraging teamwork. Quality and operational efficiency of the model significantly influences the economic and financial results of enterprises (Ginglinger, Megginson and Waxin, 2011). Ownership has quickly become an international one, electronic commerce and electronic business are already in the daily activities of a company, the new relationships with suppliers and customers have led to changes in management content and forms. One of the important challenges that must cope with the corporate governance is also optimizing IT resources such as: information, IT&C infrastructure, IT processes and associated human resources.

* AKNOWLEDGEMENT: This work was supported by the the European Social Fund **in** Romania, under the responsibility of the Managing Authority for the Sectorial Operational Programme for Human Resources Development 2007-2013 [grant POSDRU/CPP 107/DMI 1.5/S/78342].
* Mihaela Ungureanu is a PhD Candidate at Alexandru Ioan Cuza University of Iasi, Romania, Faculty of Economics and Business Administration, e-mail: myhaella5@gmail.com.

In the present context influenced by globalization, internationalization and increasingly fast growing technological development, when all goes at a speed greater than ever and the access to information must be made in real time, an organization that does not meet the current requirements of modernization has no chance to remain competitive or gain performance in a changing business environment. Information can be valuable if it help to anticipate events, to confirm or correct expectations. Access is mainly done through accounting, so that the answer to the demands of the new economic environment is the integrated accounting. Implementation of new information and communication technologies represents the condition of an efficient management system, the manager having available, any time, the necessary information for a better decision making on economic, social and environmental activity of the organization he leads (Seal, 2006).

Under current conditions, it is more and more necessary to give information security as a discipline to ensure confidentiality, integrity and availability of the electronic assets. Today, progress is conditioned by a corporate strategy including security policy and risk management, implemented in the companies concerned about promoting responsible behaviour. It is also known that important strategic role of information security can be really inserted in an entity, only if top management provides its full support and commitment.

1. THE ROLE OF INFORMATION IN THE CORPORATE GOVERNANCE SYSTEM

A strong and effective corporate governance is conditioned by a well-founded information system, which operates in the most optimal conditions. Accurate and timely information define the reliability of the capital market. The fundamental concept in this respect is that of transparency, since investments are preceded by the requirement to provide a fair image of the company, so that investors be able to take knowingly decisions. Lack of trust forms a barrier to investment, leading to a high cost of capital and reducing the efficiency of resource allocation. Information and transparency provides to all stakeholders the best economic and also managerial performance assessment, the analysis results decisively influencing the future behaviour. An efficient informational system support those interested to know and analyse the performance of a sector, through the activities and results at entity level. The new economy exploits more and more the best practices on ethical standards governing the relationships between various business partners (Armstrong, Guay and Weber, 2010).

New technologies, through the modern communication possibilities that they provide, ensure effective information, fair and transparent. Because this is managers' responsibility, corporate governance is developing like a solution to their delimitation of the company owners, as the interests of both sides are often different. Shareholders search for high profits and dividends, a rigorous control over the decisions of managers, while the latest ones want a higher decision and negotiation power, remuneration and other financial benefits, for example, participations in firm's capital.

Accounting pursues many objectives that can be achieved in various ways, but the basic one is to provide complete and accurate information to all interested parties, where financial reporting has an essential role, so that one can speak, again, about the importance of transparency. Over time the awareness about the role of accounting for the present and future of an enterprise and business environment as a whole has increased. Regulatory authorities in the field claim that a high quality of information, especially financial ones, allows stakeholders to make better investment decisions and informed choices (Auger and Lander, 2008).

From the perspective of investors, the need for accurate information takes into account elements such as accuracy, consistency, adequacy, completeness, clarity, convenience and timeliness. The relatively low level of attention that many entities attach to explain the accounting policies of restatement of incorrect information is worth noting. There are situations where the market may request details of the involved accounting issues, to prove if and to what extent the government has intervened in handling information.

Regulations on financial reporting were decisively influenced by the processes of globalization and internationalization. IASB standards directly affects the reports from the end of year, but indirectly occur during the period (eg., contracts are developed in the spirit of compliance with accounting requirements, especially regarding risk transfer) (Chaney, Faccio and Parsley, 2011).

Accounting depends on the flow of information used by each entity in part in preparing its annual accounts and a critical evaluation of the accounting policies requires a transfer of information between organizations. Voluntary information is reliable if efficiency goals such as improving the liquidity of capital markets firms, reducing its costs and if they can be used by financial analysts. Managers develop an opportunistic behaviour when there is no control on company's information disclosure.

Accounting responsibility enhances the governance system, not only by streamlining the market functions, but also by reducing monitoring costs. When the executive respects the principles

of a proper, responsible and transparent accounting, are offered premises for introducing and applying the best strategic decisions for the interests of the parties involved in. Into a developed company, accounting responsibility, and also global governance are dispersed at subunits. The entity, as a whole, cannot be responsible if its subunits are not. So, improving overall responsibility requires that in each subunit exists transparent decision making and financial reporting processes, independent audit and internal control. Also, responsible accounting promotes the exchange of information and communication throughout the company. One cannot speak about good corporate governance in the absence of effective information and communication systems. Information is the key in making profit forecasts, designed to meet market expectations regarding the company performance. If the corporate governance systems provide valuable and relevant information that analysts can include in their predictions, then it will be seen as an improvement in forecast quality and reduce dispersion (Armstrong, Guay and Weber, 2010).

If a company has effective mechanisms of governance, it must identify a problem before the proper occurrence, which involves the ability to collect, process and evaluate information. Therefore, institutional investors should seek the creation of control systems for all companies held in the portfolio, in order to facilitate the initiation of changes necessary to correct potential deviations found in strategic actions. In this sense, systems for processing information are necessary which should be evaluate existing strategy and set the desired long-term actions. If the current strategy deviates from what is desired in fact, changes could be initiated by interventions and pressures on managers.

2. INFORMATION SECURITY – PREMISE AND CONSEQUENCE OF ITS PROGRESS

It can be said that information on business has, especially in the current context, an important role in most companies and therefore, the efforts to protect it should have an important match. So, the risks that affect the information in terms of IT infrastructure are carefully discussed. This is because information technology (IT) has evolved a lot in a short time, having already an integrated part of the storage, processing and transmission of data on the organization's valuable assets. However, data security is no longer considered just a technical problem but also a concern for top management, the board and even the legal environment.

The rapid development of the Internet has led the world to the new economy. Moreover, together with the information technology revolution, the importance of knowledge as assets of the

enterprise it has increased. It creates value for a business due mainly to intangible assets such as knowledge. Most studies show that they can be classified as tacit or explicit. The tacit ones are individual experiences, known only by the person concerned, and those explicit are officially articulated and documented. In organizations, knowledge is included in archives, documents, business processes, practices and rules. It is generally accepted that they result from the accumulation of information through experience, communication or inference. In addition, such activities are dynamic, subjective, created by social interactions dependent of people, community and organization.

Economic entities are put in the situation to share held information sources in a much more open way with those interested. So, information has become exposed to three fundamental elements including: firstly, the technology used in processes of storage, processing and transmission; secondly, the stakeholders accessing information through various private networks and Internet; in the third place, the techniques for handling data as part of an organizational operation or service. Information has an important role in supporting the operations of economic entities. Each of the elements mentioned has the potential of a very real risk on the assets. So, that information to provide further support in business activities, several key features should be complied, including: *confidentiality, integrity and availability* (Chaney, Faccio and Parsley, 2011).

Confidentiality involves protecting sensitive information from unauthorized disclosure or interception. In other words, they should not be allowed to anyone who would like to access them. Only those who receive specific authorization may obtain the information. To ensure confidentiality must be clearly established that information which must be protected by a classification in public, secret and top secret information, and also setting who has access to them and to what extent. This involves the protection mechanisms for the existing information in computers and networks.

Integrity requires maintaining the accuracy and the complexity of information, given its essential role in decision making. If it is not accurate or complete, it could lead to wrong decisions of the executive, but also undesirable situation within the organization which otherwise could have been prevented. Thus, integrity aims to ensure that stored data cannot be altered or updated only by authorized persons. Control access rights must be doubled to control change, to avoid malicious intentions of those authorized to use that data.

Availability is conditioned by the guarantee that information resources are available for use at the right time. Ensuring the availability is particularly important because, without timely information, an organization would be unable to continue normal activity. In other words,

availability means that data stored in computers can be accessed anytime, from anywhere, by authorized persons.

Information security constitutes a guarantee of confidentiality, integrity and availability of electronic assets. So, it is understood that internal controls are based on information security as an integral part of corporate governance, even indirectly. However, in many companies, top management does not assume any commitment and responsibility for information security, making very difficult to support it wide to the entire economic entity. Usually management sees this problem of concern to the technical department, so it denies responsibility.

Security management of informatic systems is an important part of integrated management, which aims to create tools for risk analysis and implementing solutions to mitigate their effects in the system. The importance of the organizational components arises from the increasingly numerous and varied causes generating security problems, and also from the growing dependence of organizations to their own informatics systems. Inadequacy or lack of security measures and incomplete documentation contribute to the occurrence of security risks that may be of a human or technological. Between the major threats one can speak of fraud, theft, through which confidential data is taken from inside the company against costly advantages, poor security breaches, and failure to workstations or unauthorized use that can lead to alteration or destruction of information. Security controls are included in the general controls aimed at verifying user access to the system through their identification, authentication and authorization.

3. IT GOVERNANCE

A corporate culture based on ethics and efficiency, encourages integrity and openness, striking a balance between those elements with reasonable levels of risk. A sustained governance of information technologies helps organizations to ensure continuity and, above all, promotes strategic management of IT to gain competitive advantages. For this purpose, companies will have to improve communication between IT department and internal and external auditors.

Corporate Governance Task Force (2004) states that "the road to information security goes through corporate governance". This means that organizations establish their own safety direction by implementing the information security policy as part of an internal controls set and guiding principles that include the general framework of corporate governance system.

By providing an optimal level of security, the company imposes a responsible behaviour in terms of risk management, reporting and accounting quality, based on decisions taken by the Board

and CEO. As noted above, the term used to describe how such concerns are integrated into all policies of liability of the company, is the *information security governance*.

Information security governance characterizes a broader management strategy of the entity commencing from the Board, noting that senior management support is crucial to the success of efforts. Development of some private networks and wide use of Internet companies have facilitated trade operations with suppliers, customers, creditors and other stakeholders. With development of information and communication technologies, organizations can expand their business and markets. Moreover, even members of staff have real time access to information and applications they need for daily professional activities. Therefore, the use of new technologies has helped to respond to stakeholders constantly demands for a far better access to services and information organization (Ginglinger, Megginson and Waxin, 2011).

IT governance is part of the general system of corporate governance. The organization must know, understand the IT system architecture, the portfolio of applications and computing resources, and the role of managers in decisions regarding the organization's IT sector. IT governance must be broadly accepted as the work of management and coordination of informatics activities in an organization. It primarily concerns linking strategy and IT objectives with the strategy and economic objectives of an enterprise, then organizing informatics processes in a generally accepted model and integrated to the entity. From this perspective, IT governance obliges management to be involved in strategic decisions of this sector, particularly through investments. It also provides participation in strategic decisions of shareholders, business partners, suppliers or customers and functional departments within the company. In this way, the situation in which the solely responsible for the inadequate decisions to be only the people from informatics department is prevented.

Computing environments in countries with extensive experience in the field have developed and introduced a series of international standards including the methodologies, guidelines and procedures for certification of quality systems of the organizations whose function is related to IT&C. The most known organism is ISACA (Information Systems Audit and Control Association), which proposed the SISAS standard (Statement of Information Systems Auditing Standards*)*. IT Governance Institute has published a series of standards on the definition and implementation of controls in the systems, consolidated in a guide, *Guidelines and Procedures for Audit and Control Professionals* which has become the CobiT standard (Control Objectives for Information and related Technology). Another important organism, IFAC (International Federation of Accountants), has proposed the ISA standard (International Standards on Auditing) and IAPS standard

(International Auditing Practice Statements). The literature also presents other standards, such as SAC (System Audatibility and Control) published by the Institute of Internal Auditors Research Foundation or the standard Internal Control-Integrated Framework (Dong, 2012).

The King Report provides clarification on the need to integrate information into the security governance policies. First, an important point of view is that the Council has responsibility to shareholders; therefore, it must ensure that the organization produces value and provides an adequate return on each investment individually. In this regard, the executive management and board should develop a security policy to demonstrate their commitment to these issues and support the company's mission, objectives and strategy for information security. This approach will introduce the idea of responsibility in the three central aspects of corporate governance, namely: *people, processes and technologies*.

The specialized literature notes as main objective of IT governance, the following aspects:

- Aligning IT activities with the requirements of organizational processes;
- Supporting maximize the benefits;
- Using informatics resources responsibly, respecting the principles of efficiency and effectiveness;
- Appropriate and proper administration of informatics risks;
- Evaluating performance and increasing the added value.

Planning the information system must be understood just as production planning, in that it must set future goals, resources and expected benefits. It also be found if there is a strategic and operational plan of the enterprise information system. The strategic plan should include directions for developing the system in the long term, while the operational plan has a horizon of activity up to three years. In these plans the IT objectives correlation with economic objectives of firm is found, such as linking investments in information technology with the development of a company's electronic business.

The information system organization should consider establishing duties and responsibilities as organizational chart, posts and relationship of subordination, coordination and collaboration, and clarification of budget issues, expenses, efficiency indicators. Managerial duties related to information security can be structured on top management and executive management. Persons who are included in the first category have as main tasks (Armstrong, Guay and Weber, 2010):

– Establishing the strategy and safety policy and define a profile of risk assumed;
– Establishing responsibilities among employees involved;
– Defining values related to risk awareness;

– Managing investments and reporting security implementation schedule efficiency.

Executive management has as obligations:

– Design and implementation of safety policy;

– Identify threats, vulnerabilities and applicable practices;

– Identify available resources, priorities and measures that organization can afford;

– Conduct periodic revaluations and tests;

– Shall ensure that security is an integral part of organization life cycle processes and details each phase separately.

Information technology can play a crucial role in monitoring the effectiveness of internal controls over financial accounting system to achieve a healthy internal control environment. Integration of information security in corporate governance helps to consider such a policy as one of the fundamental operations of an organization and imposes responsibility, in terms of risk management, reporting and executive responsibility within that entity. The term used to describe how information security is seen as part of a responsible governance system of an enterprise is the information security governance (ISG). Implementing an ISG framework has several advantages for the organization, most notably the strengthening of a responsible behaviour. Among these benefits the internal security and control practices, promoting self-government and involving local authorities for law enforcement are also found.

Some theoreticians and practitioners of business environment stated that the informational resources are the "lifeblood" of an organization. A range of safety controls can be defined as an appropriate combination of physical, technical and operational forms, which provides reliable information exchange. Proving this helps a company to build trust with its partners, which in the long term, will be reflected in increased cash flow and profitability. In conclusion, there is a clear need to emphasize the importance of information security and its integration into a general program of governance. Applying a framework of responsibility and information security can generate several benefits, such as internal security practices and controls and the promoting a self-governance system.

CONCLUSIONS

The implementation and use of information systems in an organization current activity highlights, along with controls system implemented, the issue of risks which faces the informatics

system and their impact on the whole entity. IT function may be essential in an entity, by providing support for achieving strategic objectives. In this respect, it will seek to increase the automation of all activities in order to achieve expected efficiency, reduce technology costs, minimize IT risks, and ensure security and reliability of the information system. Technology was long considered only a factor to assist an organization strategy, but under the conditions of current business environment, it becomes an integral part of this strategy.

IT governance integrates and institutionalizes the best practices that support involving information system into achievement of the enterprise's objectives. In this way, by exploiting efficient and operative the information provided by system, the company maximizes its benefits, capitalizes the business opportunities and achieves competitive advantages. To obtain effective and efficient governance is necessary to implement a control framework of activities/processes as required IT standards. Since there is no theoretical guidance for setting overall IT vulnerabilities and threats, because no methodology cannot make full use of a inventory resulting from best practice experience. Application of some controls ensures consistency of IT processes, prevention and elimination of disruptions caused by erratic changes with consequences on information system reliability. Credibility can be placed into uncertainty and sabotage by malicious products, revenge or to unfair competition.

So, in order to meet requirements of the business environment in which an enterprise activates its management must understand the need and importance of information security as part of leading. Protecting information and their communication should be the responsibility of everyone involved in organizational processes, mainly managers, not only the IT department employees. This involves in fact integrating information security into the overall corporate governance of an enterprise – implementing the concept of IT governance.

REFERENCES

Armstrong, C., Guay, W., Weber, J. (2010) *The role of information and financial reporting in corporate governance and debt contracting*, Journal of Accounting and Economics, Volume 50, issue 3, pp. 179-234.

Auger, K., Lander, G. (2008) *The need for transparency in financial reporting: Implications of off-balance-sheet financing and inferences for the future*, Journal of Accounting & Organizational Change, Volume 4, issue 1, pp. 27-46.

Chaney, P., Faccio, M., Parsley, D. (2011) *The quality of accounting information in politically connected firms*, Journal of Accounting and Economics, Volume 51, issue 2, pp. 58-76.

Dong, S. (2012) *Decision execution mechanisms of IT governance: The CRM case*, International Journal of Information Management, Volume 32, Issue 2, p. 151.

Ginglinger, E., Megginson, W., Waxin, T. (2011) *Employee ownership, board representation, and corporate financial policies*, Journal of Corporate Finance, Volume 17, Issue 4, p. 873.

Seal, W. (2006) *Management accounting and corporate governance: An institutional interpretation of the agency problem*, Management Accounting Research, Volume 17, Issue 4, p. 392.