An Information Security Governance Framework

Article *in* Information Systems Management · October 2007

DOI: 10.1145/1655168.1655170 · Source: DBLP

Adéle Da Veiga
University of South Africa
28 PUBLICATIONS **550** CITATIONS

Jan H. P. Eloff
University of Pretoria
148 PUBLICATIONS **2,285** CITATIONS

Information Security Governance Framework

Eijiroh Ohki
Professor
Faculty of Informatics
Kogakuin University
eohki@cc.kogakuin.ac.jp

Yonosuke Harada
Executive Research Director
InfoCom Research, Inc.
and Professor
Osaka University
harada@icr.co.jp

Shuji Kawaguchi
Senior Project Manager
Information Security Research Group
Mitsubishi Research Institute, Inc.
kawaguti@mri.co.jp

Tetsuo Shiozaki
General Manager,
Information Security Center, Security Solutions Unit,
Fujitsu Limited
shiozaki@jp.fujitsu.com

Tetsuyuki Kagaua
Associate Professor
Graduate School of Commerce and Management,
Hitotsubashi University
cc00591@srv.cc.hit-u.ac.jp

ABSTRACT

Many companies, especially Japanese companies, have implemented information security with bottom up approach, starting from implementing piece by piece security controls. As increase the number of information security incidents and spread its impact, companies have implemented many measures in the wide spectrum, from technical counter measure systems (firewalls to protect internal network) to security management.

Japanese government has introduced compliance schemes for protecting privacy data and computers from illegal access. In addition, Ministry of Economics, Trade and Industry (METI) proposed private companies to enhance information security governance capabilities with the tools such as "Information Security Report Model" (here after IS for 'Information Security'), "IS Management Benchmarking" and "Business Continuity Planning Guide (BCP)".[6] IS Management System (ISMS) certification, IS Auditing and IS Rating scheme are also introduced to assure the implementation of security.

Then, there are so many measures existing separately. Corporate Executives (CEO and board of directors including CIO, CRO, and CISO etc.) have come to know the amount of investment for security measures is too large to pay.

This paper propose Information Security Governance (here in after, ISG) Framework which combines and inter-relates many existing information security schemes. With this ISG framework, Corporate Executives can direct, monitor, and evaluate IS related activities in a unified manner. [1]

Categories and Subject Descriptors

K.6.4 System Management: Information Systems Management System and its Governance, K.6.1 Project and People Management : Board of Directors and Executives responsibility and accountability, K.6.5 Security and Protection:

WISG'09, November 13, 2009, Chicago, Illinois, USA.
Copyright 2009 ACM 978-1-60558-787-5/09/11...$10.00.

General Terms

Management, Measurement, Security, Standardization

Keywords

Governance standards, formal governance models, formal audit models, governance architecture and implementation, risk management

1. Introduction

Rapid increase of computer and internet utilization in these two decades brought the Information Society. Companies and organizations have been eagerly utilizing computers and internet for business. At same time, misuse of computers and illegal conducts are increasing with the growth of computerization. IT ability has become to store several gigabytes of data in a finger size USB stick which can store more than million privacy data. Once such data has been exposed, many people will be suffered with spam mail, direct sales telephone and so on. Nowadays, we have seen Corporate Executives of the company are apologizing to the victims once the company exposed their information.

Information security incidents often influence to the corporate processes and operations directly. For example, if company develop and operate global value chain, they have to share information assets broadly with their business partners. Definitely, they need a secure system to share information assets to build and maintain their competitiveness. We should understand that information assets management should be a major element of business strategy, and information security measures are directly connected with the corporate value.

In addition, our business activities deeply depend on IT infrastructure. Therefore, any IT accident (for example, business process interruption by system trouble, or the leakage of confidential data of the partners) may cause a great loss to the company. There is a research that the news of IT accidents significantly reduced the company's market value. [4]

On the other hand, disclosing IS related risk information is expected to suppress negative reaction in the stock market. There is a research to compare one company that disclosed its IT risk through its financial statements with the other one that didn't disclose it. The research indicated that both stock prices reduced right after the IT accident, but the stock price of the company, who disclosed the risks in advance, returned to the original level after several days, while the other remained low for a long time. [5]

It is important for Corporate Executives to take this situation into consideration, and to review risk management processes from the viewpoints of the information security. But most executive regards the corporate information security measures as the administrators' matter. Most of the companies have implemented measures for Information Security with bottom-up approaches. The systematic measures like ISMS are spreading, but the executives sometimes don't have awareness of risks and measures that should be shared with administrators and employees. In this situation, it is difficult for the executives to carry out its accountability on information security risk.

In Japan, a study group, sponsored by METI, had started efforts to develop the concept of ISG. In 2005, the group made a model of "Information Security Report"[6], a tool for a corporate to explain its information security policy and related activities to stakeholders, like a model of Corporate Social Responsibility report (CSR report). METI has recommended this model to the companies. Some companies published their Information Security Reports. According to the brand assessment in an industry that handles security products, the percentage of user companies who positively evaluate firms that disclose a report on information security has increased significantly since 2006.[7]

The study group also designed a concept of "Information Security Management Benchmark" [8] to provide reference data for enterprises to make sound decisions on measures and investment of information security. The ISM-Benchmark is a self-assessment tool to visually check where the level of the company's security measures resides, by responding questions about company profile and 25 items of security measures. The number of accumulated records exceeded 17,000.

In addition, METI made a guideline for Information Security Audit, in 2003. [7] [9] There are more than 10,000 companies and organizations during a year that use Information Security Audit.

In this paper, we propose new ISG framework for Corporate Executives to overcome difficulties around ISM, and make clear the relationships among ISG and related tools and programs.

2. Requirement for ISG

As we discussed our background in previous section, in most cases corporate information security programs had started from bottom to up. Started from the workplace, from piece by piece security control mainly focusing on technical solution necessary to protect departmental information assets, based on workplace risk assessment conducted by department staffs. Later, most organizations became to understand that there should be effective management mechanism in place to coordinate these controls to get more sophisticated outcomes.

Gradually, most organizations became aware of the fact that these sets of bottom-up security programs might not be able to solve the difficulties and issues surrounding information security. Even if they have management mechanism to coordinate these controls, they will not be effective enough without clear alignment and interconnection between the management mechanisms and corporate governance mechanism.

In addition to these management mechanism, ISG, Information Security Governance, has become recognized to be a key portion of corporate security program, requested as a part of corporate governance framework.

The word "ISG" has become familiar these days, but almost nobody clearly knows the functions of ISG and differences between ISG and ISM yet. Most difficulties and issues remain unchanged.

From the Systems engineering perspective, ISG is, of course, a system composed of several elements; each element has interrelationships with other constituent elements, and pursues common objectives as a whole. Difficulties and issues, we face to govern Corporate Information Security, are suggesting that we may be missing any key element of ISG, or missing key interfaces between elements of ISG.

To recover these missing element and interfaces, and to make governance system more effective, we would better have ISG framework, an overall picture of ISG, in which all critical elements explicitly defined with functions of each element, and interfaces among elements. The framework is a kind of theoretical model that clearly show the structures and mechanism how ISG works, and Corporate Executives can understand how they can map these functions and interfaces to their actual organizations.

It can be easily understood that IGS framework and its function model must satisfy following three key requirements.

Requirement #1: ISG framework and function model should be consistently constructed with other corporate risk governance framework so that executives can make decisions easily and effectively, since information security is one of the major corporate risk areas, and management of information security risk also should be a part of corporate risk management framework.

Requirement #2: At same time, ISG function model also need to be capable to handle unique characteristics of information security risk which are essentially different from other risk categories. Mainly these essential characteristics come from the differences between BIT and ATOM. BITs can be easily copied, transmitted and shared around the globe instantly. Information sharing with specific business partners may bring huge business advantage, but at same time, single security incident may lead to total business failure. IGS functional model needs to be capable to govern risks in such fierce circumstance.

Requirement #3: ISG functional model should be able to include existing information security management and control mechanism, such as ISMS, and be able to have effective interface with the elements of these existing mechanism.

3. Reference model for ISG

3.1 Relation between Corporate Governance, IT Governance and ISG

Corporate governance includes all aspect of governance to deal with every risk. Similar to the fact that corporate executives are responsible for the corporate governance, they are also responsible for both ITG and ISG. The relation between ISG and ITG is not clearly defined, although information security is one of big topics in ITG. ISG includes not only IT security but also physical security and paper security. Thus the relation with ISG and ITG is shown in Figure 3.1. [1], [3] One example of the intersection of ITG and ISG in Figure 3.1 (IT security element) is that a computer access control system which identifies the accessed personnel by ID and password and permits him to access to protected data according to his assigned privilege. Most of automated security controls belong to this category.

The other examples of non-IT of ISG in Figure 3.1 are paper security and physical security. Paper may be printed out by use of IT. However, paper is still used for hand written evidence for a contract, an approval of purchase, and an entry form into a secured server room. Those papers are stored safely and protected. A rule for paper handling is within the responsibility of executives. Physical security is another example of non-IT where only restricted personnel can enter into the secured area. Executives may ask to implement IT to restrict access to the room with IC card and automated door.

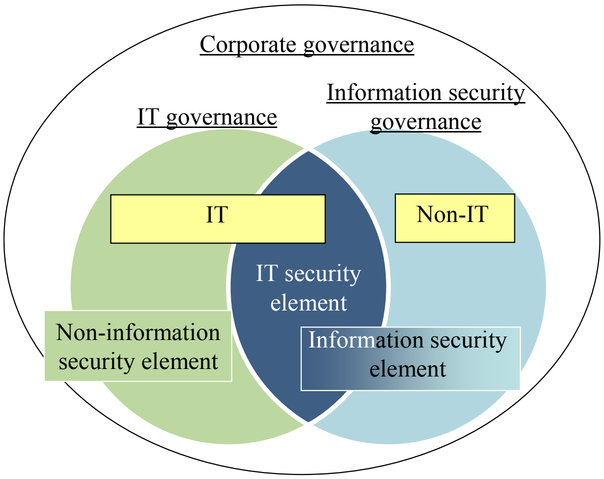
Corporate governance
IT governance
Information security governance
IT
Non-IT
IT security element
Non-information security element
Information security element

Figure 3.1 Relation between ISG and ITG

3.2 Configuration of the ISG framework

ITG framework has been discussed in ISO/IEC 38500:2008. As we have stated that ISG has common integral part with ITG, ISG should be aligned with ISO/IEC 38500:2008[10]. We propose a new extended model for the ISG framework in Figure 3.2 based on three requirements stated in chapter 2.

The new model consists of five components, three common parts with ISO/IEC38500; "Direct" for guiding managements from the viewpoints of business strategies and risk management, "Monitor" for ensuring the governance activities visible with measurable indicators, "Evaluate" for assessing and verifying the results/outcomes. We extended with two new components for Information security aspect; "Oversee" for observing and auditing governance processes, and "Report" for disclosing the report to the stakeholders (see Figure 3.2).

As shown in Figure 3.2, the framework includes the governing cycle starting from "Direct," "Monitor," and "Evaluate" Information Security Management (here in after ISM) process. Because ISO/IEC 27001:2005[11] requires "commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS", the ISG framework should incorporate with this requirement.

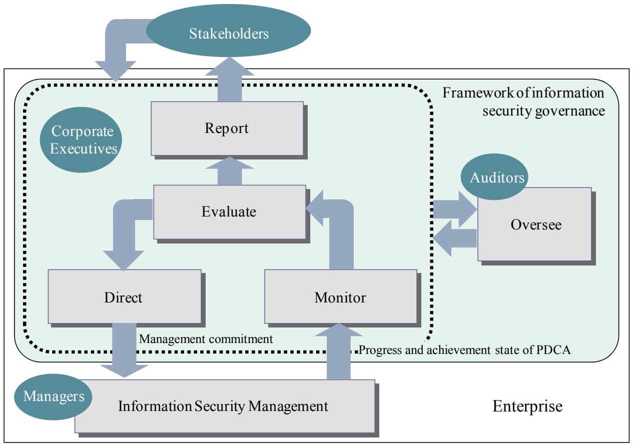
Stakeholders
Framework of information security governance
Corporate Executives
Report
Auditors
Evaluate
Oversee
Direct
Monitor
Management commitment
Progress and achievement state of PDCA
Managers
Information Security Management
Enterprise

Figure 3.2: PROPOSED FRAMEWORK OF INFORMATION SECURITY GOVERNANCE

Note that the stakeholders may select the company as a business partner or an investment target while taking its ISG activities into consideration, but stakeholders is not included in the framework model because they are not controllable.

3.3 "Direct" in the ISG framework

Information security incident response requires quick decision and action to reduce dames or losses on information asset. "Direct" in the ISG framework ensures good interaction between executives and the management to implement good ISM, communication and preparedness against potential risks. Implementation of "Direct" for ISG is different from that of ITG, because executives should have certain role and responsibility on ISM project. If executives think their role is just order the management, real-time response to information security incidents may not possible. For ISG, executives should understand and take combination of actions to ease the situation. It looks similar to corporate portfolio management.

"Direct" in the ISG also includes defining the scope of the ISM, formulating a risk analysis, and allocating necessary resources. Enacting "Security policy" for ISM is the responsibility of executives.

3.4 "Monitor" in the ISG framework

"Monitor" of ISG includes two functions. First function is to oversee the status of the ISMS PDCA cycle which is comparable to that of ITG. Management should check the potential risk and assess preparedness and counter measures put in place. If once the allowance exceeds the limit set by executives, they should report to the executives. Sometimes this function is automated and display to "Dash Board" designed for executives.

Second function is to surveillance of potential Information Security incident and accident. Real time "Monitor" is crucial to the security and is not necessary to ITG.

3.5 "Evaluate" in the ISG framework

For "Evaluate" process, executives analyze and measure the degree of achieving the goals from management data collected in the "Monitor" process, and take corrective action if necessary.

Major difference from ITG, ISG requires real time decision to minimize loss, error, or damage caused by security incidents. For example, in case of SQL injection attack and followed modification on corporate e-commerce web site, immediate action should be taken by the management and its impact should be reported immediately to the executives. Depending on the damage or impact to corporate business, executives should evaluate it quickly and take necessary actions on real time. Because of the nature of attacks against the internet site, it is not possible to forecast when and how. The early and appropriate response of executives is the key to ease the tension.

"Evaluate" will activate "Report" to stakeholder to understand corporate security in Figure 3.2. Nowadays, many stakeholders have strong interest in corporate security, because his stock price may be devaluated by security incident. He would ask the company to disclose the status of information security preparedness.

3.6 "Report" in the ISG framework

"Report" is also proposed to incorporate into the ITG framework because stakeholders require the transparency and accountability of Information Security. Similar to the CSR report which is used to ensure the corporate contributing society, ISG "Report" ensures the implemented security measures in corporate.

In the past, the occurrence of an accident or incident relating to information security is rather small and its impact to the society is not serious, and even such companies were not accused from the society. However, in recent years, a privacy information exposure or a service interruption due to system failure happened more frequently. Stakeholders recognize that those companies have higher risk and regard them not to trust on their business relations unless they disclose their security problems and improvement. Thus it is necessary to disclose activities for information security from an "accountability" point of view so as to avoid negative hearsay and to trust from the external stakeholders.

There are two purposes for company to disclose activities for information security to external stakeholders. The first one is to announce that the company fulfills its social responsibility by reporting practical information security activities, with security incidents if any.

The second purpose is to report activities for information security from the viewpoint of rising corporate value. These activities can increase the confidence of the partners and customers, resulting in constructing a long and stable relationship with the partners as well as in royalties from the customers. Moreover, if they implement the strategic management on information assets, then the company's cash flow may be increasing or stable in the future. As confidential information including technology and know-how, customer privacy data, and information networks configurations are strategically most important, protecting and controlling them is being regarded as an important business objective. As far as the corporations make no disclosure, they rarely receive a high rating from the investors and never obtain a resulting economic effect.

Both purposes are not always exclusive to each other. Disclosing the security related activities is very important because it has a side effect on raising information security awareness to employee. Reporting to the outside "Disclosure" can be regarded as a "promise" the company gives to the society. This is because disclosing the activities makes it possible for every employee to be aware that the "promise" to external stakeholders is important.

Information security disclosure does not mean to disclose information security vulnerability. This is because if the company disclose their vulnerability on their firewalls, company web site may be attacked and increase risk. Companies are not required to open their weakness to customers, partners, and outsourcers.

In the case of the disclosure from an "accountability" point of view, it is important to provide content that allow the receivers to check whether the information security activities are carried out as explained. The important thing is that what information security policy is developed, in what sort of information security process are put in place, and what system ensures the effectiveness is all observable. Then, disclosing item should include (1) information security policy, (2) risk evaluation, (3) risk measures and response, and (4) management system.

In the case of the disclosure from a "value creation" point of view, the important thing is what kind of economic effect it produces. The economic effect includes how much cost the information security activities reduce through making an inventory of information assets, the extent to which they increase the brand value as well as the trust of the customers and partners, what economic value protected information assets have, and how much the implementation of the activities reduces the risk of damaging the information assets. If those efforts are visible and accountable, investors can estimate the corporate value highly and the stock market may give a high price to the corporate.

According to the corporate brand assessment in an industry that handles products relating to information security, the percentage of user companies who positively evaluate other firms that disclose a report on information security has increased significantly since 2006.[6] Moreover, the former tended to give importance to the evaluation of information security activities when selecting a partner. Similarly, higher the company's attitude to information security activities is, higher the user company's satisfaction is.

Table 3.1 is the example form of Information Security Report from the trial conducted by METI in 2005. [6]

Table 1: Example of Information Security Report

(1)Basic Information

Includes the purpose of issue of the report, cautions relating to usage, target periods and responsible departments.

(2)Concept of Management regarding Information Security

Includes policy regarding information-security undertakings, target scope, ranking of stakeholders in the report and messages to stakeholders.

(3)Information Security Governance

Information security management system (e.g. placement of responsibility, organizational structure and compliance), risks relating to information security and information security strategy.

(4)Information Security Measures Planning and Goals

Includes action plan and target values

(5)Results and Evaluation of Information Security Measures

Includes results, evaluation, information security quality improvement activities, management of overseas bases, outsourcing, social contribution activities relating to information security and accident reports.

(6)Principle Focal Themes relating to Information Security

Includes internal controls and protection of personal information, undertakings to be particularly emphasized such as Business Continuity Plans, introduction to themes and newly devised points

(7)Third-party Approval, Accreditation, etc. (if acquired)

Includes ISMS compliance evaluation system, information security audits, privacy mark systems, number of persons with information security qualifications, classification and ranking.

3.7 “Oversee” in the ISG framework

“Oversee” is a kind of auditing function to check and validate Corporate Executives’ IS related activities. It is very important for every organization to check its sound operation from third party viewpoint. ISG framework will make Corporate Auditors, independent from corporate executives, feel easier to conduct IS related auditing with clearly defined functions which executives expected to perform.

4. Conclusion

New ISG model, consists of DIRECT, MONITOR, EVALUATE, OVERSEE and REPORT, occupies key position in the total ISG system, and cover the missing functions of corporate IS initiative.

Now we can clearly see the whole picture of ISG, Information Security Governance system, including existing approaches, efforts and tasks. Five key functions are clearly defined, and relationships with existing approaches are specified.

Since every function has been clearly specified, it is easy for most corporations to check their existing functions and tasks against new ISG model, and find missing element or interface if any. It is also useful for most corporations to define their functions and interfaces of their own ISG, depending on the physical organizational structure and role and responsibility sharing, referring this New ISG Model.

It is obvious that new ISG framework and function model satisfies three key requirements discussed in section 2. ISG framework has similar functional architecture with ITG, and relevant to be consistent with other risk management framework. Each element has designed functionalities to deal with unique characteristics of information security related risks, and identical interfaces with the elements of existing ISM mechanisms.

We strongly recommend that this New ISG Model is almost indispensable for every corporation and organization to coop with quickly changing world in Information Society. Information Related Risk is one of the corporations’ key risk areas to be governed and managed under the sophisticated mechanism.

Remaining studies should be focused on the relationships with other information security models such as risk metrics, control activity monitoring and evaluation methodologies.

It is also required to have clearly defined relationships among existing security related programs, such as ISM benchmarking, Assurance type IS Audit, ISMS certification scheme, and ISG framework. We have already started to sort out relationships among related programs in Japan.

5. Acknowledgements

Authors acknowledge to METI and following committee members and who contributed to a publication in Japan (“ISG guidance” [2], 2009).

- Satoru YAMASAKI, PMO, CISO Office, IBM Japan
- Mitsuhiko MARUYAMA, Partner, Deloitte Tohmatsu Risk Services Co., Ltd.

Authors also acknowledge to Dr. Ikuo MISUMI, Director, Office of IT security policy, METI, and anonymous contributors who support for developing the guidance.

6. References

[1] Ministry of Economics, Trade and Industry (METI), Guidance to Introducing Information Security Governance, 1st July, 2009 (in Japanese)

[2] ISACA/ITGI, Information Security Governance Guidance for Boards of Directors and Executive Management 2nd Edition, Mar. 2006

[3] E. Ohki, Framework of Information Security Governance, Japan Society of Security Management 23rd Annual conference, 2009 (in Japanese)

[4] K. Ito, T. Kagaya, Kim.K, "Information security governance to enhance corporate value", Hitotsubashi University Center for Japanese Business Studies / Working Paper No.91, Jan 2009

[5] Kim,H., "The Effects of Prior Risk Information Disclosure on Investors' Decision-Making: Using Cases of Revealed Information Leak Risks.", Hitotsubashi Review of Commerce and Management vol.2, No.2, Nov 2007

[6] METI, Report of Research Group on Corporate Information Security Governance (Overview), 2005 (http://www.meti.go.jp/english/information/data/IT-policy/pdf/report_of_information_security.pdf)

[7] METI, Information Security Auditing Guideline Version 2, 2008 (In Japanese)

[8] Information-technology Promotion Agency, Information Security Management Benchmark (ISM-Benchmark), (http://www.ipa.go.jp/security/english/benchmark_system.html), 2006

[9] Japan information Security Audit association (JASA)(http://www.jasa.jp/) (In Japanese)

[10] ISO/IEC, ISO/IEC38500:2008, Corporate governance of information technology, 2008

[11] ISO/IEC, ISO/IEC27001:2005, Information technology - Security techniques - Information security management systems - Requirements, 2005