

Risk Key

ISACA—Chennai , Issue # 2, March 1, 2009

President's column

Dear Readers

Welcome to yet another issue of the Newsletter. Though many forward looking organizations have started recognizing Information Security, as one of the business imperatives, there are many things to do beyond such recognition to sustain and strengthen initiatives that are taken from time to time on a proactive manner-A security organization to be established and nurtured, policies and procedures to specifically address issues revolving around organization need to be in place, users are to made aware of ,trained and supported with secure ways of doing things in the dynamic ,ever-changing environment, monitoring& review to be scheduled to plug loopholes and to make the system and supporting infrastructure robust, agile and resilient.....endless activities in this never ending journey.

However difficult and uphill task may be the journey, one common thread, which stitches across all the loose ends, is relevant and up-to-date knowledge. There is no substitute for knowledge; The knowledge to recognize the fact that rules of business are changing with the changes triggered by economic slowdown and consequential turmoil ;the knowledge to take into cognizance the new vulnerabilities and sophisticated attacks and threats affecting the security; the knowledge to identify and deploy cost effective solutions in an environment where cost optimization is no more a choice ;the knowledge to introduce newer and effective new initiatives-cloud computing, green-datacenters, outsourcing, (continued on last page)

Ernst & Young's Global Information Security Survey

According to the survey findings, a growing number of organizations recognize that information security can provide more than just protection of corporate assets and reveals that there exists a strong link between information security and brand & reputation.

This year's survey confirms a shift from regulatory compliance-driven information security to business improvement and stakeholder-driven information security with a strong emphasis on keeping a good brand and reputation safe from internal & external threats which can take years to build and which could be severely damaged or even destroyed by a single security incident.

The survey indicates that despite economic pressures, organizations are increasing investments in information security and more organizations in India are adopting international security standards with 58% of the respondents (Global 50%) planning to increase their investment in information security as a percentage of total expenditures.

Companies today realize that while the top line and bottom line growth needs attention, it cannot happen at the expense of security. During these difficult times a security breach can prove costly as it may cause irreparable monetary as well as reputational damages for the company.

The Global Information Security Survey which is in its 11th year gauges the current state of information security and the major

factors shaping its future interviewed 1,400 senior executives in more than 50 countries with India emerging the second largest contributor with 107 respondents. The survey indicates that most believe a security incident would have a greater impact on reputation and brand than on revenues, with 84% of respondents citing damage to reputation and brand as significant, compared with 80% for loss of revenues and customers.

Key findings:

1. Protecting reputation and brand has become a significant driver for information security.
2. Despite economic pressures, organizations continue to invest in information security.
3. International information security standards are gaining greater acceptance and adoption.
4. Many organizations still struggle to achieve a strategic view of information security.
5. Privacy is now a priority, but actions are falling short.
6. People remain the weakest link for information security.
7. Growing third-party risks are not being addressed.
8. Business continuity is still bound to information technology.
9. Most organizations are unwilling to outsource key information security activities.
10. Few companies hedge information security risks with cyber insurance

Guideline # 16- Effect of Third parties on an Enterprise's IT Controls

In this column of the newsletter you will find that we take up for discussion IS Standard, Guideline or Procedure issued by ISACA . In the current issue we take up for consideration G16 (Guideline # 16- Effect of Third parties on an Enterprise's IT Controls). This guideline originally issued on March 1, 2002 has now been reviewed and updated effective March 1, 2009. For more details and complete guideline please refer to ISACA website.

Ineffective third-party controls can weaken the ability of an enterprise to achieve its control objectives.

IS auditors should consider reviewing such things as the contract, service level agreements, and policies and procedures between the third party and the enterprise. IS auditors should obtain and document an understanding of the relationship between the services provided by the third party and the enterprise's control environment. The third party's process and controls relevant to the enterprise's process and controls should also be documented.

The IS auditor should identify and assess the risks involved with the process and determine whether the risk resides with the enterprise or the third party. IS auditors should identify each control, its location in the combined control environment (internal or external), the type of control, its function (preventive, detective or corrective), and the organization that performs the functions (internal or external) that offset or compensate for those risks. IS auditor determine the significance of third-party controls on the ability of the enterprise to meet its control objectives.

After obtaining an understanding, IS auditors can confirm their

understanding of the control environment through a variety of methods including such things as inquiry and observation and process walk-throughs. Where the role of the controls at the third party on the enterprise's Control Objective is significant the IS auditor should assess the controls. It is also important to understand the effects of the third party providers on the enterprise. This could include economic viability of the third party provider, how information is handled within their system, processing integrity, application development and change management processes. This is because lack of controls or the weakness in its design will have a devastating effect on the enterprise. Once the control weakness are identified it is necessary to assess the impact after considering its significance on the control environment and the compensating controls. In the review of the contracts the IS auditor has to ensure that roles and responsibilities are documented. This guideline elaborates on the areas that should be focused during the review. The IS auditor can also call for independent third party reports or decide to directly review and test the controls. The guideline also details the IS auditor should consider when setting the scope of such an audit including reviewing the internal audit process and reports of the third party. It is pertinent to note that the same procedure is to be followed when the third party sub-contracts any of the services relating to the enterprise. The report should elaborate the control weakness and the recommendations and suggest any compensating controls where required.

A detailed reading of the IS Standards, Procedures and Guideline will help to effectively carry out the responsibilities as an IS auditor. Further Code of Professional Ethics guides the professional and personal conduct of members of the Association and/or its certification holders.

Looking Back

Founders' Day March 7, 2009
President's Address



Special Guests- Dr.Malaviyya and Sevalaya Muralidharan



One of the Founders of ISACA Dr. M.Revathy Sriram



A section of the gathering of members



15, Ground Floor,
Luz Golden Enclave
(TNHB Complex Next to
Kamadhenu Theatre)

Telephone # +91-44- 2498 4331

Still Looking Back

Seminar on Common Criteria Certification on March 14, 2009

Hon. Secretary K.B.Sankaran addressing the gathering



Subhendu Das



Venkatasubramanian



A section of the gathering of members



Looking Ahead

It is proposed to have a one-day event on Business Continuity Management -BS 25999- Date to be decided—browse ISACA Chennai's website (www.isaca-chennai.org) for updates.

President's column (contd.)

co-sourcing, collaborative, grid computing, virtualization and many more—call it by any name; the knowledge to align security seamlessly with business; the wisdom to recognize that security is not one stop solution but a dynamic journey -of course with milestones to celebrate and reward the efforts.

One of the multiple and evergreen choices for updating such knowledge is reading. We endeavor to quench your thirst thru the chapter news-letter, which will be as informative as all of us want that to be. You may support by sharing your experience by contributions to enrich.

Anything which will add value is most welcome from any of our members/readers. The news -letter for the quarter beginning April09 is with you.

PL ENJOY AND FEEL FREE TO REVERT WITH SUGGESTIONS AND CONTRIBUTIONS FOR IMPROVEMENT.

Yours sincerely

N.S.N. Pillai

Last word

From now on we plan to write about COBIT and how it is all the more relevant in the current environment. In the first part of this series we deal with the need for control framework for IT Governance and how COBIT fits the bill.

We will start with COBIT Mission:

To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for

adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals.

A control framework for IT governance defines the reasons IT governance is needed, the stakeholders and what it needs to accomplish.

It is heartening to find that top management is realizing the significant impact the information contributes to the success of the enterprise and how IT can be leveraged successfully for competitive advantage.

Enterprises cannot deliver effectively against the business and governance requirements without adopting and implementing a governance and control framework for IT. A governance and control framework needs to serve a variety of internal and external stakeholders, each of whom has specific needs. A framework for IT governance and control should have business focus, process orientation, general acceptability, common language and help meet regulatory requirements.

IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives. *Control Objectives for Information and related Technology (COBIT®)* provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

End of Part 1

For circulation among members of ISACA only. Not for sale.

Please provide your feedback on the newsletter. It will help us to serve you better.

This issue is edited & Published by MP. Badrinath on behalf of EDITORIAL COMMITTEE OF ISACA, CHENNAI. Emani BSP Sarathy is the advisor to the Editorial Committee.