Information Protection Management

Project Overview

The topic selected by me is Information Trust and Compliance Issues (SOX) and I have chosen to cover more depth about a single application of Confidentiality of Data that is Information Protection Management. This is as per the SOX section 404 Audit that describes the importance of the IT component of internal control guidelines. Financial data must remain confidential in transit via email outside the corporate network and this involves risks of confidential information, PCI/HIPAA/SOX/SEC violation and also a huge reputation risk.

The approach that I have used is a real world application where consultants can actually use the questionnaires, risk assessment model and information protection worksheet provided by me to conduct assignments at client locations to address the problems of information protection.

My project has been linked to the lecture 5 (February 16, 2006) by Deron Grzetich from Protiviti who had spoken about the Sarbanes Oxley Act of 2002. One very interesting part that he addressed was about the IT Control and Design where he explained the issues of Authentication, Change Management and Confidentiality of Data and that is how I got interested in this particular topic. I was in touch with him and was seeking feedback and exchanging ideas with him over the course of this project.

Other than Information Trust and Compliance, my project largely covers Business Risk Management where I have developed the Business Risk Assessment Model for enterprises to assess risk. This model also deals with strategic vulnerability management and how it could be assessed using the questionnaires provided by me. Lastly, the role of critical infrastructure in information protection management has also been addressed.

The project delves into describing a variety of technical issues of incident handling procedures though there is a greater emphasis on business perspectives.

Executive Summary

Background:

The Information Protection Management Guidelines (IPMG) provides standards and guidance for all business units to utilize good information protection practices to ensure XYZ Inc.'s confidential and proprietary information, in all of its forms. Information Protection is not just an IT issue. Business managers must be fully engaged in this process.

Highlights of the IPMG:

Risk-based Approach to Information Security

The IPMG's underlying principle is to require business units to assess the risk to information from the perspective of Impact to the Company and the Likelihood of an attack against that information. The areas of exposure are unauthorized Disclosure, Modification, and Loss of Availability of information. By classifying information into Risk Levels, business units will ensure that cost of protection is justified by the severity and likelihood of exposure.

Risk Levels

The IPMG sets Risk Levels at four levels:

Level 3	Irreparable Harm to XYZ Inc, Very likely target
Level 2	Significant Harm, Possible target
Level 1	Moderate Harm, Unlikely target
Level 0	No Harm, Not a target (Level 0 applies only to risk of Disclosure)

Most of the Company's information falls into Level 0, Level 1 and Level 2. Only a small percentage of information falls into the highest risk level of 3.

Information Security Officers (ISOs)

The IPMG requires that business units assign the role of the ISO to implement the information protection guidelines.

Information Protection Control Objectives (Control Matrix)

The IPMG contains a detailed matrix of approximately 200 information security controls that are arrayed by protection level (1, 2, 3) so that low risk business processes and IT applications need only apply baseline controls (approximately half the controls). These controls are detailed enough to provide specific guidance to ISOs and IT professionals for proper information protection, and are consistent with best practice and internationally recognized information security standards (ISO standard 17799). The controls include detailed standards in areas of password policy, auditing and logging, authentication, confidentiality, network security, third party and remote access, standards for vendors, temps, and consultants, and other relevant areas. The controls matrix is the security standard for all IT assets, infrastructure, and applications, as well as for business processes within which information is systemically used.

Information Protection Plans (IPP)

IPPs are in essence remediation plans. ISOs are responsible for developing IPPs for their business units, and implementation of the applicable controls. Corporate Security has developed a web based software utility to assist ISOs in plan development, including the automated selection of applicable controls based on risk levels.

Compliance

Corporate Internal Audit is responsible for auditing business unit compliance to the IPMG. A waiver process is available where controls cannot be applied due to technological or compelling business reasons.

CIT and IT Groups

CIT is responsible for providing the technical infrastructure and IT security services to secure the enterprise and assist divisional IT groups in meeting the IP Control Objectives. Thus, IT groups are able to select the security services necessary to adequately and cost effectively protect business unit information, as defined by the protection levels assigned by those business units.

IPMG IMPLEMENTATION PHILOSOPHIES

As XYZ Inc. continues to work toward its objective, its reliance on proprietary information and intellectual property shall continue to grow at almost exponential rates. XYZ Inc. might be faced with the challenge of articulating information access and protection policies that find the best balance between information sharing and information protection. In addition, we need to define implementation plans that smoothly incorporate those policies into the data management practices in place at each site worldwide.

The IPMG promotes three core philosophies as a basis for achieving the proper balance of control of and access to information:

- Look at information protection as an ***information driven*** process. While core information systems are critical, XYZ Inc.'s proprietary information must be protected in all its forms and during all business activities. This means that how we protect information in our offices and at offsite locations is just as important as our system access controls, userids and passwords.
- Information protection is not a one-time event; it will be a way of life at XYZ Inc. The IPMG must be implemented as a process. It must be part of the decision-making processes related to organizational, business process, information system and facilities planning life cycles.
- Effective information protection requires effective communication. Information Owners are responsible and accountable for ensuring that the information they create, maintain and use is properly secured based on industry best practices and statutory and regulatory

requirements. Because of XYZ Inc.'s complex business processes and partnerships, many employees and contractors would create and modify copies of core information in the context of their jobs in ways that are not easily monitored by information owners. An effective implementation of the IPMG requires discussions between departments and across business functions to ensure that all copies of information are correctly assessed as to risk and vulnerabilities.

Information systems personnel are often asked to accept the Information Security Officer (ISO) role. However, the ISO's responsibility touches information in all forms, including physical hardcopy, verbal communications, etc., and in all venues such as meeting rooms, off-site conferences, etc. Therefore, it is essential that ISO's have the authority and executive management support to implement effective security awareness and incident response programs to compliment the IPMG Program.

<u>CORE INFORMATION SECURITY OFFICER (ISO) FUNCTIONS</u>

The Information Security Officer role should be vested with business line and/or IT employees who understand how the business line generates and uses information. This knowledge helps the ISO facilitate good information protection controls. The following table provides a template for integrating IPMG roles and responsibilities into a business line context:

Table 1 – Roles and Responsibilities

Information Security Officers

- Establish information protection programs within the business unit in accordance with Corporate Policies, Corporate Security programs and divisional policies/directives;
- Work with business units in developing risk-based, cost effective information protection plans (IPP);
- Refer information security incidents to Corporate Security for investigation and assist in investigations, where appropriate, by preserving evidence with assistance from local IT and/or site security personnel;
- Coordinate implementation of adequate physical and computer security measures to safeguard information and equipment (including routine inspection of offices to ensure information is properly secure); and
- Provide Business Unit Management with periodic updates and assessments of IPP

implementation.

Business Unit Management

- Appoint Information Security Officers (ISOs)
- Sponsor ISO programs to classify information in all of its forms;
- Establish budgets and funding for Information Protection Plans, incident response and security awareness programs.

Divisional IT Organizations

- Work with respective business units in developing and implementing an IPP that includes time lines, milestones, and costs for implementing baseline standards, and
- Coordinate with CIT and Corporate Security to develop a business line oriented catalog of information security technology services covering information protection for all appropriate media and data processing situations.

Corporate Security

- Formulates corporate policy, standards and guidelines on information protection;
- Assists business units and IT organizations in implementing information security programs;
- Coordinates and supports Information Security Officers;
- Provides assistance for developing IPPs and information classification programs;
- Promulgates information protection awareness and training; and
- Conducts vulnerability assessments and security investigations, including primary contact with law enforcement regarding information security and intellectual property incidents.

CIT

- Develops a catalog of security products and services in support of enterprise-wide IT operations; and
- Implements appropriate risk-based, cost-effective, and efficient security services to protect the enterprise infrastructure and information traversing the infrastructure.

Internal Audit

- Reviews business unit IPPs during the regular audit cycle.

Security Awareness Basics

An employee and contractor population that has been informed about security best practices and possible threats might greatly decrease XYZ Inc.'s exposure to disclosure, modification and loss of sensitive and critical information. Information Security Officers will find that they get a lot of value from implementing even a basic security awareness program.

An effective security awareness program has at least three key components:

- New employee orientation awareness materials,
- Periodic but continual awareness messages in media such as web newsletters, special communications (e.g. current virus attack information) and other communications that exploit current events to get a security message out; and
- Presentations to business groups in venues such as poster sessions, staff meetings, conferences, etc.

Incident Handling Procedures

Information security incidents come in all sizes and many varieties. Virus attacks, email chain letters, computer and data theft, improper use of email or the INTERNET, hacker intrusions, and denial of service attacks are just a few of the incidents that may harm XYZ Inc., its employees and business partners. No matter how complex, incidents generally fall into two categories based on their potential impact:

- ***Contained Incidents*** - where the impact is known, contained and manageable. Examples include complaints about email content/chain letters, computer thefts without intellectual property loss, etc., and
- ***Major Incidents*** - where the potential scope of harm is unknown, is not easily containable, or where XYZ Inc.'s corporate reputation, productivity and/or revenue is at risk. Examples include a major virus attack, hacker intrusions, and thefts of XYZ Inc.'s intellectual property.

Depending on the type of incident, different XYZ Inc. departments may need to coordinate to effectively investigate, contain and recover from the event. In cases where XYZ Inc. employees or contractors are alleged to have done something wrong, Corporate Security and the site Human Resources groups should always be brought onboard as soon as possible to lead an investigation. Depending on the site, the Site Security department should also be contacted. For technical threats, such as viruses, the appropriate CIT representative should be contacted as soon as possible along with divisional IT groups as required.

ISOs should assess their site's readiness to handle *contained* and *major* incidents. If necessary, ISOs should recommend that an incident response program be established for major incidents. At a minimum, response plans should ensure that activities adhere to the following principles:

(a) Immediately contact the appropriate local incident response personnel;

(b) Assess the severity of the incident;

(c) Take good notes (4 w's - who, what, when, where) and store notes securely;

(d) Notify the right people (e.g. Corporate Security, legal, HR, IT, etc.);

(e) When investigating, ensure that evidential integrity is maintained to help ensure court admissibility;

(f) Enforce a need-to-know policy and strive to protect employee and company privacy;

(g) Communicate incident information securely (e.g. encrypted email, land-lines opposed to cell phones, etc.);

(h) Contain the problem (i.e. prevent from getting worse);

(i) As required, ensure a backup of the affected system & assess & perform backup of involved or impacted information as required;

(j) Perform a root-cause analysis and prevent the problem from happening again; and

(k) Get back into business (i.e. ensure that backups have not been compromised, restore, and resume business activities).

As a general rule, disciplinary actions related to incidents involving XYZ Inc. employees must be coordinated through the site Human Resources Department and in conjunction with business management. Lastly, roles and responsibilities for key individuals responsible for executing an incident response plan should be clearly defined and documented.

ISO Checklist for Identifying, Retrieving and Preserving Evidence

- Strict compliance with best evidence practices may not be possible in all instances, especially when there are urgent business needs to get a computer or network back online. If it is necessary to depart from best practices, the reason for doing so should be documented so that a reasonable response can be given to potential legal questions that may arise at a later date.
- Whenever possible, evidence should be preserved in its original form, and it should be handled and maintained in a manner that will prevent it from being altered.

- The key to determining what is evidence, and what is not, is to think in terms of what it will take to demonstrate to someone with no prior knowledge of the effected computer or network, what occurred and how it occurred.
- Hard drives containing original evidence should not be booted under any circumstances prior to making an image copy and preferably not at all after an image was made.
- Whenever possible, "hot Swappable" hard drives should be available to facilitate retrieval of evidence and restoring online services.
- Any and all directories and log files should be retrieved that would be necessary for the reconstruction of events.
- Computer evidence should be hand carried to Corporate Security whenever possible, but when that is not practical, it should be shipped via overnight delivery service.
- A chain of custody record should be maintained with the evidence.
- Each item of evidence should be marked with the initials of the person submitting it and the date it was preserved.
- A list identifying all people having access to the evidence should be sent to Corporate Security along with the evidence.
- Consult with your local XYZ Inc. attorney to resolve any conflicts between any procedures described herein and local laws.

For more detailed information about evidence handling see Appendix, Guidelines for Identifying, Retrieving and Preserving Computerized Evidence.

MANAGING THE INFORMATION PROTECTION PLANNING PROCESS

Information Security Officers must establish an overall plan to implement the Information Protection Management Guidelines. Performing the following three-step process will result in a completed Information Management Model (IMM) and Information Protection Plan (IPP) for the department, division or other area under review.

STEP 1: Establish the scope and depth of required analysis

- Identify major business functions (at a business line, division, and/or department level).
- Identify information domains within each business function (i.e., each Information Domain consists of one information object, its users, systems and security policies)
- Identify/inventory application systems within domains (in some cases the domain is made up of one or more application systems used to store and/or process the information object in that Domain).
- Prioritize domains/systems based upon initial perceived risk.

STEP 2: Determine domain/system risk and control details

- Establish the business owner for each domain/system.
- In conjunction with the Domain/System Owner, assess seriousness and likelihood (S & L) of Disclosure, Modification, and Loss and document the business rationale for the resulting S & L ratings. Appendices provide additional guidance regarding impact and threat assessment to guide management's analysis of seriousness and likelihood of loss. Also refer to the IMM model displayed after Step3.
- Put the S & L ratings into the Information Protection Worksheet (IPW) to obtain required protection ratings for Confidentiality, Integrity, and Availability (CIA).
- Define the technical details for the domain/system(s) that describe how information objects are input, stored, processed and output as a basis for understanding what controls are or should be in place
- Perform a controls analysis, i.e. detailed questions plus evidence, as you feel necessary, on the domain/system in question to see if it has the necessary controls (based on CIS Control Matrix) for the CIA protection ratings determined above.
- Prepare a gap analysis for each domain/system in question relating to the CIS Controls Matrix versus existing controls.

STEP 3: Determine overall control gaps, implementation objectives and action plans

- Prepare an IPP based on the domain/system gap analysis including cost of implementing required controls and specific timelines for implementation. The IPP can be implemented by domain or at the IMM level as desired by business management and according to economies of scale.
- Obtain the authorization of the Business Unit Manager to proceed with IPP implementation. If management will not authorize all required controls then obtain a waiver and send along to CIS for review and approval.
- Implement the IPP.
- Monitor and re-assess as necessary, but at a minimum when major changes occur in the business function, organization, systems or facilities supporting the business functions in the IMM.

<u>Corporate Security Information Management Model (sample)</u>

Table – Corporate Security IMM

Key: D=Disclosure, M=Modification, L=Loss
C=Confidentiality, I=Integrity of information, A=Availability of information

Information Object	Data Owners	Authorized Users	Applications	Servers/ Systems	Seriousness			Likelihood			Protection Level		
					D	M	L	D	M	L	C	I	A
Investigations	Corp Security	All members of Corporate Security	Case Mgmt Sys Email/Exchange Hard copy files Text files	Legal Notes Server #1 Exchange Paper files PCs/laptops	3	1	1	3	1	1	3	1	1
Corporate Security Project and Budget	Steve Nyman, Corp Security	Directors in Corporate Security	Project Tracking System (Oracle) Email/Exchange Hard copy files Text files	Legal Oracle server #2 Exchange Paper files PCs/laptops	2	1	1	1	1	1	1	1	1

Information Protection Plan

The writing of the IPP is a “gap analysis” between the state of security of the current systems versus the justified protection rating for each. The IPP that you develop will include the security measures you deem appropriate based on the degree of protection indicated in the IMM. During this process, you may determine that certain types of information and their systems are not appropriately protected (over protected or inadequately protected). In many cases, the current state of security as determined during development of the IMM, will be adequate. The gap is the current state of security controls implemented versus the controls described in the Information Protection Management Guidelines and the Controls Matrix.

There is no required format for the IPP. It is suggested that you develop the IMM as above and then select the security measures that will most cost effectively manage your risk, documenting the plan to implement in a way that is best suited to your operations. Systems that are common to many of your information domains such as the LAN, desktop computer hard drive, email, paper files can be grouped together in the IPP. They do not need to be discussed over and over with each domain.

Table – Sample IPP for Corporate Security Information

Information Object	Authorized Users	Applicatio n	Servers/ Systems	Confidentiality	Integrity	Availability	Security Status & Plan

Information Object	Authorized Users	Application	Servers/ Systems	Confidentiality	Integrity	Availability	Security Status & Plan
Investigations (investigation notes, evidence, and disposition information)	All members of Corporate Security	Case Mgmt. System (Lotus Notes application)	Legal Notes Server #1	PROTECTION VALUE=3 1. Annual audit & review of the db 2. OS & db logging on 3. Create sensitive file area 4. Authentication via application pswd, increase to 7 characters, force change monthly, 12 month history, 5 attempt lockout 1 hour 5. annual awareness statement w/ esign	PROTECTION VALUE=1 6. Software change control 7. data edit/delete restricted to 2 admins 8. NT server logging all logins and failed logins	PROTECTION VALUE=1 9. database backed up to tape daily, off site storage	Items 3,4,5 to be implemented by end of Q2 2001. Other items in place
		Text & data files	Laptops	1. BIOS passwords, 7 characters 2. Auto screen savers 10 min w/ pswd 3. Hardrive encrypt w/ Win2000	No change	4. labeled w/ name & address	Win 2000 limiting encryption implementation. Item 1,2 & 4 1Q01
			desktops	1. Remove domain	1. disallow local login by non-admin		coordinate w/ Legal IT on impact

Information Object	Authorized Users	Application	Servers/ Systems	Confidentiality	Integrity	Availability	Security Status & Plan
				Users frm C$ Sharing hard Drive	users		
Corporate Security Project and Budget tracking	Directors in Corporate Security	Project Tracking System (Oracle)	Legal Oracle server #2	PROTECTION VALUE=1 1. Passwords changed every 90 days 2. Min password length=6 3. Password must be different than last 3 passwords used.	PROTECTION VALUE=1 Software change control NT server logging only failed attempts	PROTECTION VALUE=1 database backed up to tape by CIT	All security services implemented

Conclusion and Findings

Based on the various guidelines and models provided, a consultant can actually implement this at a client location and derive the following findings as per the IPP process.

Description	Process	Tools	Deliverables
Understand the business functions, key players and systems to estimate the work and schedule meetings.	Define Scope	IPP Estimating Model & Timeline	Scope Definition
Determine the overall risk to an enterprise if its information were disclosed, modified or lost in an unauthorized manner.	Assess Risk	IPP Risk Questionnaire, Impact Assessment Guidelines	Information Management Model
Identify areas within existing systems or manual processes where the information is not being protected as required.	Conduct Gap Analysis	Control Matrix	Gap Analysis
Create a plan addressing vulnerabilities to keep an enterprise safe	Complete IPP Action plan	Catalog of Security Services	Action Plans
Stay focused on keeping the Information protected during system or organizational changes.	Maintain IPP	IPP Utility	Documented Change Control

Annotated References

www.protiviti.com
www.bearingpoint.com
www.capgemini.com
www.deloitte.com
http://www.sec.gov/news/press/2005-134.htm
http://www.pcaobus.org/Standards/index.aspx
http://www.aicpa.org/info/sarbanes_oxley_summary.htm
http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
www.issa.org/gaisp/_pdfs/strawman_mapping.pdf
www.isaca.org/cobit