DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING

Introduction

- Organisations are **increasingly relying on IT**. It is presumed that the information required is available all the time, **it is accurate, it is reliable** and no unauthorised disclosure of the same is made.
- Additionally, virtual business organisation is up and running all the time on **24×7 basis.**
- However, in reality, the technology-enabled and technology-dependent organisations are vulnerable to Security threats. E.g. denial of service attacks, virus, cracking, hacking

Why is Information System Security Important?

- Besides many direct and indirect benefits, there are also many **direct and indirect risks relating to the** "information systems". These risks have led to a gap between the "need to protect systems and the degree of protection applied". **This GAP is caused by:**
- Widespread use of technology
- Unevenness of technological changes
- Interconnectivity of systems (e.g. Internet)
- Elimination of distance, time, and space as constraints
- External factors such as legislative, legal, and regulatory requirements or technological developments

THREATS TO INFORMATION SYSTEM

- **May arise from intentional or unintentional acts and may come** from internal or external sources. The threats may **originate from, among others:**
- Natural disasters (fires, floods)
- Environmental conditions (electrical surges)
- Technical conditions (program bugs, disk crashes)
- Human factors (lack of training, errors, and omissions)
- Unauthorized access (hacking)
- Viruses
- Other threats, such as business dependencies (reliance on 3rd party, outsourced operations, etc.)

What Is Information System Security?

- **Security relates to the protection of valuable assets against loss, disclosure, or damage. Safeguards** include-
- Physical safeguards for securing valuable assets from threats, sabotage, or natural disaster. E.g. locks, perimeter fences, and insurance are common
- Logical and Technical safeguards. E.g. user identifiers, passwords, firewalls
- **Concept of security applies to all information.**

Security Objective

- The objective of information system security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of **confidentiality, availability, and integrity** (CIA)”.
- For any organization, the **security objective is met when:**
- **Confidentiality**: Data / information are disclosed only to those who have a right to know it
- **Integrity**: Data and information are protected against unauthorised modification
- **Availability**: Information systems are available and usable when required

What information is sensitive?

- **Business Operations: They consist of an organization's *process and procedures, most of which are*** deemed to be proprietary. As such, they may provide a market advantage to the organization.
- E.g. A company's client lists and the prices charged for various products and services can be damaging in the hands of a competitor.
- Most organizations prohibit the sharing of such data. However, carelessness such as inadvertent storage of data on unauthorized systems, unprotected laptops/media results in compromise.

What information is sensitive?

- **Strategic Plans: Most organizations readily acknowledge that strategic plans are crucial to the** success of a company.
- But do most companies really make an effort to protect these plans?
- E.g. A competitor learns that a company is testing a new product line in a specific geographic location. The competitor removes its product from that location, creating an illusionary demand for the new product. Based on the positive but false marketing results, the company decides to roll the product out nationwide. It discovers that competition for its new product is intense. Result: multi-million dollar loss as sales falter.
- Above example illustrates that keeping strategic plans confidential is essential.

What information is sensitive?

- **Finances:** ***Financial information, such as salaries and wages, are very sensitive and should not be*** made public.
- E.g. As salaries and wage-related charges normally comprise the majority of fixed costs, lower costs in this area contribute directly to an organization's profitability. When a competitor knows specific information about a company's wages, the competitor may be able to price its products accordingly. When competitors' costs are lower, they can either under-price the market or increase profits. In either case, the damage to an organization may be significant

Protecting Computer-Held Information Systems

"*how to protect the information systems*",

- **Rule #1: Know what the information systems are and where these are located.**
- **Rule #2: Know the value of the information held and how difficult it would be to recreate if it were** damaged or lost.
- **Rule #3: Know who is authorized to access the information and what they are permitted to do with the** information.
- **Rule #4: Know how quickly information needs to be made available should it become unavailable for** whatever reason (loss, unauthorized modification, etc.)

Protection that an organization can use:

- **Preventative Information Protection: It is based on use of security controls. Information** system security controls are generally grouped into three types of control:
- Physical: Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems
- Logical (Technical): Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems
- Administrative: Security Awareness, User Account Revocation, Policy

Protection that an organization can use:

- **Restorative Information Protection: Security events that damage information systems will happen. If** an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business.
- Planning & operating an effective & timely information system **backup and recovery program is vital.**
- Few questions any restorative information system protection program must address:

  Has the recovery process been *tested recently?*

  How *long did it take?*

  How much *productivity was lost?*

  Did everything go according to *plan?*

Protection that an organization can use:

- **Holistic Protection: Protection of corporate information systems from harm or loss must be done** holistically (-global/macro level-) and give the organization the appropriate level of security at a cost that is acceptable to the business.
- One must plan for the unexpected and unknown, expect the worst events to happen, and recover from these events if and when they occur. Such events can't be planned, and they tend to happen at the most inopportune times. It is inappropriate to wait until the last minute to decide on a protection plan and recovery process

Information Security Policy

- A **Policy is a plan or course of action, designed to influence and determine decisions, actions and other** matters.
- A **security policy is a set of laws, rules, and practices that regulates how assets including sensitive** information are managed, protected, and distributed
- An **information Security policy addresses many issues such as CIA concerns, access rights and related** procedures, separation of duties, controls, ownership and authority issues

Information System Policy?

- **User Security Policy: sets out the responsibilities and requirements for all IT system users. It provides** security terms of reference for Users, Line Managers and System Owners.
- **Acceptable Usage Policy: sets out terms for acceptable use of email and Internet services.**
- **Organisational Information Security Policy: sets out the Group policy for the security of its** information assets and the Information Technology (IT) systems processing this information. It is THE MAIN IT security policy document.

Information System Policy?

- **Network & System Security Policy: sets out detailed policy for system and network security and** applies to IT department *users*
- **Information Classification Policy: sets out the policy for the classification of information**
- **Conditions of Connection: sets out the Group policy for connecting to their network. It applies to all** organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

Security Organisation Structure

- **Information Security Forum (ISF): Forum includes GSO, AGSO(Ass. Group Security Officer), and senior representatives from every** division.
- Role- to ensure that there is clear direction and visible management support of security initiatives within the organisation.
- **Information Security Management Group (ISMG): This cross functional group includes AGSO,** Divisional System Security Officer (DSSO) from every division, IT Security Officer (ITSO), and the Personnel and Facilities Management Security Officers.
- Role- to co-ordinate the implementation and management of information security controls across all of the divisions and sites.

Security Organisation Structure

- **Group Security Officer (GSO):**
- Role- overall responsibility for security within the Group. This includes the security of all information assets, the network accreditation scheme & for non-IT security including physical & personnel matters.
- **Assistant Group Security Officer (AGSO): Reports to GSO, ISF.**
- Role- to co-ordinate the implementation and management of information security across the Group.

Security Organisation Structure

- **IT Management:**
- Role- overall responsibility for security of the IT infrastructure.
- **IT Security Officer (ITSO): Reports to the ISMG on IT security matters.**
- Role- to manage IT security programmes and IT security incidents.
- **Facilities Management Security Officer (FMSO): Reports directly to Facilities Management on all**
- security matters relating to personnel.
- Role- to ensure that the controls are implemented, adhered to and reviewed as necessary.
- **Installation Security Officer (ISO): ISO appointed for each IT environment.**
- Role- responsible for all security matters related to their system/installation and/or network and will

Security Organisation Structure

- **System Security Officer (SSO): SSO appointed for major application system(s).**
- Role- to focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
- **Divisional System Security Officer (DSSO): A System Security Officer (SSO) from each division will be**
- appointed as a DSSO.
- Role- Same as a SSO; to represent the SSOs in their division at the ISMG and communicate requirements and issues to/from this group.
- **Personnel Security Officer (PSO): Reports directly to Personnel Management and the ISMG on all**
- security matters relating to personnel.
- Role- to ensure that the controls set out are implemented, adhered to

Security Organisation Structure

- **System Owners: Role- overall responsibility for the information security of their own systems.**
- Responsible for allocation of protective markings to their systems and data according to the Information Classification policy. Delegating day-to-day operational aspects of live systems.
- **Line Managers: Role- to ensure compliance with the aims and objectives of the policy. To ensure** that all required security measures are understood and in force.
- **Users: Role- to comply with the security procedures for their system and any applicable general IT** security guidance.

Audit Policy

- **PURPOSE of the IS Audit policy**
- To provide **guidelines to the audit team to conduct an audit on IT based infrastructure system.**
- The Audit is done to ***protect entire system from the most common security threats which includes the*** following:
- Access to confidential data
- Unauthorized access of the department computers.
- Password disclosure compromise
- Virus infections
- Denial of service (DoS) attacks
- *Open ports, which may be accessed by outsiders*
- *Unrestricted modems- unnecessarily open ports*

IS Audit Reports

- **Structure: The components of an audit report are discussed below:**
- **Cover and Title Page: Audit reports should use a standard cover, with a window showing the title,** the department's name, report's date of issue, and names of the audit team members. Some of these items may be repeated at the bottom of each page.
- **Table of Contents: The table lists the sections and sub-sections with page numbers including** summary and recommendations, introduction, findings (by audit field) and appendices (as required).
- **Summary / Executive Summary: It gives a quick overview of the salient features- main issues** covered,

IS Audit Reports

- **Introduction: It should not repeat Summary details. It should include the following elements:**
- ***Context: It briefly describes conditions in the audit entity during the period under review E.g.*** the entity's role, size and organisation especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organisational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.

IS Audit Reports

- **Purpose: It is a short description of what functions and special programs were audited and the** clients' authorities
- **Scope: It lists the period under review, the issues covered in each function and program, the** locations visited and the on-site dates
- **Methodology: It briefly describes sampling, data collection techniques. basis for auditors'** opinions, any weaknesses in the methodology

IS Audit Reports

- **Findings: It constitutes the main part of an audit report. Results of examination of audit issues in the** context of established objectives and clients' expectations.
- **Opinion: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do** so as per the requirement.
- **Appendices: Appendices helps in understanding the report. They usually include comprehensive** statistics, quotes from publications, documents, and references.
- **Level of Detail: The depth of coverage for issues should normally reflect the significance of the** findings. Situations representing a high degree of risk or indicating shortcomings that are serious enough to justify a recommendation should be treated extensively.
- Specific initiatives should be described in detail, while issues which are general in nature or where the department meets the expectations should be dealt with briefly.

IS Audit Reports

- **Commentary: Where a "recommendation and a compliment" are made under the same issue, they** should be in separate paragraphs; otherwise, they may confuse the reader and reduce the impact of one or the other.
- **Statistics need to be used consistently throughout the report. Sample size and error rate mean more** when they are given in context. The size of the population, the number of transactions and the period of time provide that context.
- **Percentages should not be used when referring to small samples (<100).**
- **Graphics should be used when they add to the understanding of the text.**

THANK YOU