



# Managing Information Security: The Perspective of CIOs

*CT Yong, Zainurrijal Abdullah, SN Lo, Nazree Ghani, BD Lim*

Universiti Brunei Darussalam



## *Agenda*

- ◆ Roles and Responsibilities
- ◆ Management as Dominant Component
- ◆ Begins with Planning
- ◆ Establish Security Programs: C.I.A.
- ◆ Components of a Security Program
- ◆ Security Management Models
- ◆ Way Forward

## *Roles & Responsibilities*

- ◆ Who is chiefly accountable for Info sec?
- ◆ CEO, CIO, CISO, CTO, COO?
- ◆ Most firms put CISO >> CIO >> CEO
- ◆ Drawbacks of Infosec Manager reporting to CIO:
  - a) limited authorities & access to resources,
  - b) may conflict CIO needs to optimise usage
- ◆ Any structure is better than no structure! There should be a single focal point for managing Infosec
- ◆ Such roles must be documented and communicated across the organisation. Note that information security deals with the physical and environment security too.



## *Management as Dominant Component*

- ◆ Managing infosec is liken managing key resource
- ◆ Minimum generic approach: Plan, organise, lead, control
- ◆ CIO gets involved in shaping & translating strategies
- ◆ Resources & processes aligned to strategies & operations
- ◆ Additional characteristics must be addressed: IT cuts across all functions, dynamic in terms of temporal, distribution, values
- ◆ Includes managing physical security & social behaviour



## *Begins with Planning*

- ◆ Planning calls for investigation/ identification of:
  - ◆ Needs of information for business growth
  - ◆ Types of usage & users classification
  - ◆ Risks and vulnerability
- ◆ 3 Components of contingent plans:
  - ◆ Incidence Response Plan: indicators and process
  - ◆ Disaster Recovery Plan: relative to service levels
  - ◆ Business Continuity Plan: activate hot/warm/cold site
- ◆ Guided by Policies:
  - ◆ Enterprise Information Security Policy
  - ◆ Issue specific security policy
  - ◆ System specific Policy

## *Establish Security Programs: C.I.A.*

- ◆ Fundamental aspects of Infosec:
  - ◆ Confidentiality: privacy, levels of access, authentication
  - ◆ Integrity: system for ensuring data quality & relevance
  - ◆ Availability: protected system for supporting data flow
- ◆ Tied back to org. structure & processes
- ◆ Clearly defined roles & responsibilities
- ◆ Procedures for preventive, alert, patching, intrusion, audit trails, access to the premise and information system
- ◆ Committed to security education & awareness
- ◆ CIO must define data owners, custodians, users
- ◆ Measures also consider past employees, customers, contractors, outsourced services

## *Components of a Security Program*

- ◆ Policy: Define the Program, Issue Specific & System Policies
- ◆ Program Management: Central Security & System Level Programs
- ◆ Risk management: Risk identification, assessment, mitigation
- ◆ Life Cycle Planning: from initiation to disposal of security plan
- ◆ Incident handling: incident detection, reaction, recovery
- ◆ Personnel and Staffing: define user administration
- ◆ Awareness and Training: types of promotion and alert
- ◆ Physical Security: guards, gates, locks, logs, alarms
- ◆ Logical Access control: identification, authentication, criteria
- ◆ Audit trails: systems logs, log review process
- ◆ Encryption: Types, VPN, contractors, outsourced services
- ◆ Security Education Training and Awareness Plan

## *Security Management Models*

- ◆ ISO 17799 Part 1: Code of Practice for Information Security Management
  - ◆ Organisation that implements the ten sections to satisfaction of an auditor will receive ISMS certification
  - ◆ 1) Organisation Security Policy, 2) Security Infrastructure, 3) Asset Classification and Control, 4) Personnel Security, 5) Physical & Environment security, 6) Communications & Operations, 7) system Access control, 8) System Development & maintenance, 9) Business Continuity Plan, 10) Compliance
- ◆ National Institute of Science & Technology (NIST) Security Models,
  - ◆ SP800-12: The Computer Security Handbook- categorise three aspects of controls (management, operational and technical)
  - ◆ SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems - as listed in previous slide
  - ◆ SP800-26: Security Self Assessment Guide for IT Systems-based on the three aspects controls to determine the level of achievement

## *Security Management Models*

- ◆ Information Systems Audit and Control Foundation-COBIT ( Control Objectives for Information and Related Technology): Gaining lots of support in US and covers 12 items:
  1. System Documentation Review- that documentation is adequate
  2. Utilities Review- that all utilities are restricted to authorised users
  3. System Security Review- that controls can prevent unauthorised usage
  4. System Environment Control Review- that operating system holds all users and processes in a controlled environment
  5. Remote Access & Communication Review-that dial-up and network users are properly controlled
  6. Review of Interfaces with other OS- that multiple operating systems if used can retain the control over the system resources
  7. Software Modifications Review-that all modifications are tested, documented and performed according to established procedures
  8. Automated Logs Reviews- that logs are produced, reviewed and stored
  9. Error Handling Reviews- that system handles information on error resolution
  10. System Backup Review-that backup system is put in place
  11. Administrative Control Review-that separation of duties is adequate
  12. Security Software Review- that the security software used provides control

## *Way Forward*

- ◆ CIO may decide to adopt a standard practice and seek certification if business requirements call for such measure
- ◆ Most organisations would best perform incrementally by focusing more on using IT to drive business growth instead of security and controls
- ◆ CIO may get squashed when some security breach occurs if no visible measure or security due diligence is in place
- ◆ CIO needs to constantly educate management and colleagues that risk is inevitable and costly to eliminate completely
- ◆ CIO may adopt a hybrid approach of balancing resources for maximising IT usage and implementing security controls
- ◆ CIO should start with the soft approach of managing information security ie at the management and operational aspects (physical access control, passwords, allocate resources for training and putting a secure infrastructure)