

Class Two

Topics:

- Security in Organizations
- Security Policies
- Security Awareness vs Training
- Basics of Information Classification
- The Incident Response Team

8/23/2007

Class 2

1

Basics of Management

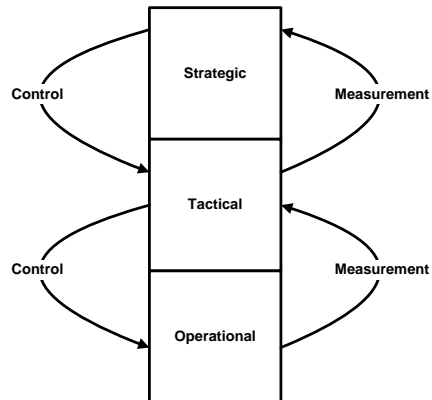
- Components of Management
 - Mission
 - Goals
 - Objectives
- Tools of Management
 - Policies
 - Planning
 - Procedures
 - Standards

8/23/2007

Class 2

2

Organizational & Management Levels



8/23/2007

Class 2

3

Governance and Information Security Management

- Governance: That which directs and controls the organization in order to achieve the organization's goals
- Governance requires
 - Internal control systems
 - Alignment of organizational activities with organization's mission, goals, and objectives
- The IT Governance Institute (ITGI) provides recommendations for information security governance, including:
 - Involvement of governing board in setting policy and allocating resources
 - Independent assurance via audit
 - Business input into policies and practices
 - Concern with entire IT lifecycle

8/23/2007

Class 2

4

Information Security involves many areas of the enterprise

- Information Technology
 - Security Administrator
 - Technical Systems Administrator
 - User Support
- Internal Audit
- Facility Security
- Records Management
- Human Resources

8/23/2007

Class 2

5

Role of Information Security Administrator

- Establish Standards
- Administer and implement security measures
- Disaster recovery planning
- Consults to other areas regarding IS security
- Develop user and system administrator manuals for security
- Keeps upper management apprised of security issues, especially new legal and regulatory measures
- Works with internal and external auditors
- Vendor relations
- Liaison with government, industry, and nonprofit security organizations

8/23/2007

Class 2

6

The Security Policy

- Criteria for making security decisions :
 - Who makes decisions about security,
 - what processes do they follow,
 - what goals are they trying to achieve
- Important to governance
- Links business requirements to security practices
- Ensures accountability for security
- Protects business assets
- Ensures common expectations about security

8/23/2007

Class 2

7

There is more than one "Security Policy"

- Corporate Policy
 - Management's security statement
 - General goals, not specific standards (should specify individual accountability for systems use, should not actually define password length)
 - Sometimes called an organizational or program policy
- Functional policy
 - Deals with a specific issue of concern, such as email use, laptop encryption, etc.
- System-Specific Policy
 - Policies that apply to a specific system or application
- End User
 - Collection of issue policies pertinent to organizational end users
 - Internal – Employee, Contractor
 - External – Customer, Vendor
- It's OK to have multiple "Security Policies" as long as their specific context is clearly understood

8/23/2007

Class 2

8

Elements of a Security Policy

- Definition of information security
- Statement of management intent to support security
- Definition of terms
- Definitions of responsibilities
 - Generic to security function (e.g., data owner, custodian, user, etc.)
 - Specific to enterprise organization structure (e.g., executive management, IT security administrator, end users, etc.)
- Specific Policy Statements
 - Who is responsible for what
 - What is and is not compliance
 - How will policies be enforced
- Policy Maintenance
 - Who can change the security policy
- How often or when will this be done

8/23/2007

Class 2

9

Obtaining End User Compliance (How to ensure a policy works)

- Visible executive commitment
- Hold managers accountable for compliance in their area
- Ongoing education and awareness
- Ensure policies and procedures are workable
- Ensure consistent compliance and enforcement
- Make users sign statement of policy compliance
- Take action when the policy is violated

8/23/2007

Class 2

10

Role of Security Training and Awareness

- Difference between awareness and training
- Training components
 - Build knowledge and skills
 - "How to do"
 - Important for technical staff, also HR, Internal Audit, etc.
 - Technical training must include current awareness of security alerts and bugs
- Awareness Components
 - Change attitudes and beliefs
 - "What to do"
 - Awareness of your own practices
 - Awareness of other's possible violations
 - Necessary for all employees, technical and non-technical
 - Should emphasize ethical side of security

8/23/2007

Class 2

11

Security Awareness Programs

- Important Hints
 - Security Awareness is a sales pitch
 - Know your audience
 - Keep it simple
 - Take advantage of current events
 - Get feedback, measure results, change course if need to
 - Emphasize improvements and positive feedback
- Consider:
 - Videos
 - In-house newsletter
 - Computer-based training
 - Contests
 - Games
 - Posters
 - Trinkets
 - Classroom style lectures
 - Screen saver messages

8/23/2007

Class 2

12

Security & the Human Resource Function

- Hiring
- Performance Evaluation
- Awareness and Training
- Job Descriptions (documented responsibilities)
- Confidentiality Agreements
- Methods to Handle Legitimate Grievances
- Employee Termination
 - Alert the gatekeepers
 - Timing is critical
 - Ensure safety nets
 - Inform all vendors
 - Be cautious with terminated employee's associates
 - *Legal Issues*

8/23/2007

Class 2

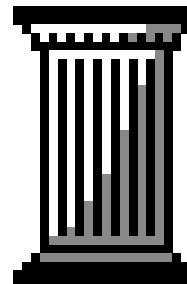
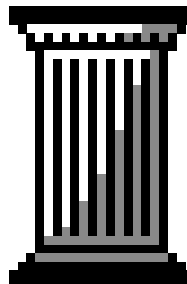
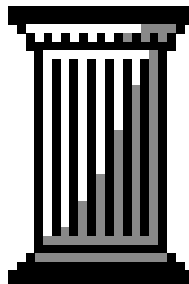
13

The 3 Pillars of Security

Classification

Need to Know

Separation of Duties



8/23/2007

Class 2

14

Department of Defense Classification Levels

- Unclassified
- Sensitive Unclassified
- Confidential
- Secret
- Top Secret

Basis for classification is documented in DoD 5200.1-R, which may be found in <http://web7.whs.osd.mil/text/d52001p.txt>

8/23/2007

Class 2

15

A Possible Commercial Classification Scheme

Public	Specifically cleared for publication – press release, marketing material, etc.
Company Confidential	Any employees who has signed the usual confidentiality agreement
Proprietary	Only those specifically authorized
<i>Proprietary may include the following:</i>	
Trade Secret	Only those specifically authorized
Privacy Protected	Only the individual concerned and other authorized individuals, per legal protections over privacy
Executive Confidential	Executive, Legal, the Board of Directors, anyone with specific fiduciary responsibility

8/23/2007

Class 2

16

Classification and "Need to Know"

- Higher Classification = higher losses from disclosure, therefore more expensive security is justified
- Higher Classification implies:
 - Physical restriction on hardcopy data
 - Limited distribution to those properly cleared
 - Stronger protection of stored and in-transit data
 - Destroyed data is unreadable (paper shredder, de-gauss magnetic media)
- Inference Upwards and Downwards:
 - Downwards - inferring more highly classified details from less classified summaries
 - Upwards - inferring more highly classified summaries from less classified details (e.g., Traffic Analysis)
- Need to Know:
 - Restriction on access within a classification level
 - Horizontal organizational controls vs. vertical controls implied in classification
 - Both classification and need to know are required to access data

8/23/2007

Class 2

17

Requirements for a Classification Scheme

- Security Policy
- Marking or labeling of data
- Procedures to control access to data, based on labels
- Procedures controlling retention and disposal of data
- Controls for compliance tracking
- Procedure for downgrading or de-classifying data
- General Requirements:
 - Accountability
 - Assurance (the system works)
 - Continuous Protection (the system works all the time)

8/23/2007

Class 2

18

Incident Response Functions

- Preventive: Keep security incidents from happening
 - Correct vulnerabilities in vendor products, as they become known
 - Educate users and technical support on good security practices
- Reactive: Treat serious security breaches as a "fire alarm" event
 - Provide mechanism for internally reporting and acting upon incidents. Create visibility to upper management on security breaches.
 - Work with legal and criminal investigative groups. Preserve trail of evidence for possible prosecution.
 - Treat serious security breaches as a type of emergency or disaster affecting corporate assets and functions. Protect critical business functions, and ensure timely recovery in the event of an incident. Minimize damage to organization.
 - Determine what future countermeasures may prevent similar incidents from recurring

8/23/2007

Class 2

19

Incident Response Team (IRT) Functions

- Create and staff incident hot line
- Manage and report on incidents
- Maintain contacts with investigative agencies
- Assess seriousness of any reported breach
- Administer counter-measures
- Initiate system recovery, if needed
- Deal with the press and other media
- Provide a liaison with vendors for problem reporting and fixing
- Provide a liaison for outside incident response teams
- Generally functions in an advisory role (as opposed to site Security Administrators)

8/23/2007

Class 2

20

Considerations in Forming an Incident Response Team

- Defining the constituency
- Advertising the services
- Identifying trusted contacts
- Establishing trusted communication paths for incident reporting
- Ensuring no information is released without proper permissions (e.g., security vulnerabilities)
- Staff management
- Defining IRT internal security policies
- Review legal considerations (e.g., monitoring network traffic in the course of an incident, etc.)
- Reporting, trend analysis, correlating reports of similar intrusions across many targets
- Developing an incident database
- Community education

8/23/2007

Class 2

21

External Incident Response Teams

- CERT - Computer Emergency Response Teams
- CIAC - Computer Incident Advisory Capability
- FIRST - Forum of Incident Response and Security Teams
- AusCERT - The Australian CERT

AusCERT publishes an excellent guide to starting an incident response team at :

http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html

NIST also has Special Publication 800-61, Computer Security Incident Handling Guide:

<http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

8/23/2007

Class 2

22