Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Enterprise Roles

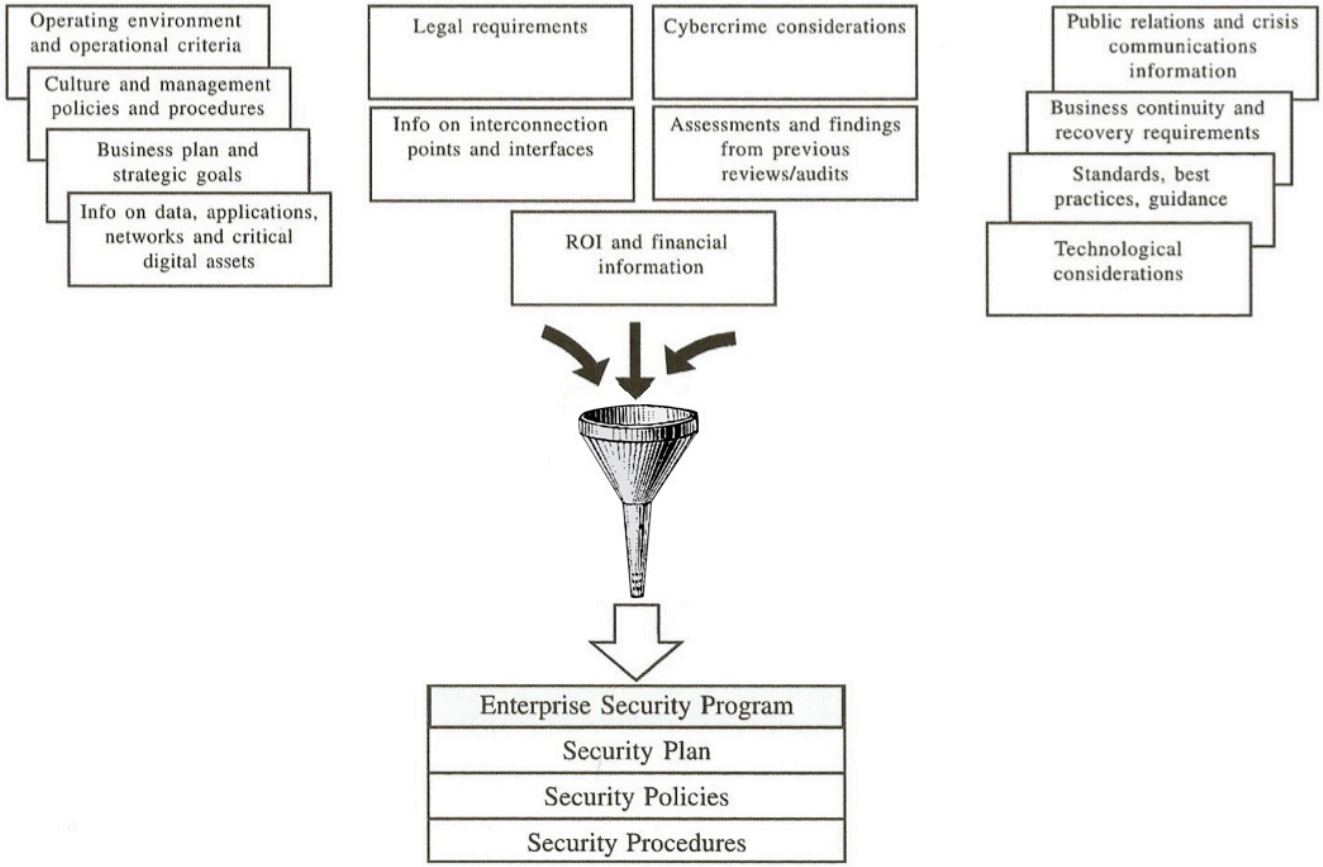
510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 8

Enterprise Security Approach

- Multidisciplinary responsibility
  - Managerial
  - Operational
  - Technical
  - Legal
- Avoid stovepipe view

ESP Input

Figure 1-3: Input into an Enterprise Security Program



From *Roadmap to an Enterprise Security Program*

Elements

- Risk management
- Security plan
  - Procedures
  - Controls
- Implementation
- Audit

Challenges

- Educate constituencies
  - Need for enterprise approach
  - Interests and requirements of other groups
- Identify and develop processes
- Develop cross-department links
- Foster team approach
- Address turf problems
  - Question knowledge
  - Question skills
  - Question understanding

Elements

- Networks
- Applications
- Information
  - Digital
  - Analog

P6STN1

- People
- Products
- Plants
- Processes
- Policies
- Procedures
- Systems
- Technology
- Networks
- Information

Evaluate all with multidisciplinary approach

The Process

- Security Plan
  - Strategic document
- Security Policies
  - Broad statements that account for management's risk tolerance and expectations
- Security Procedures
  - Actual steps in the security process
- Controls
  - Standards for each element

Development Stages

- Governance
- Security Integration and Operations
- Implementation and Evaluation
- Capital Planning and Investment Controls

Governance

- Risk management decision makers
- Operational management staff
  - Cross-organizational teams
- Inventory assets
- Establish ownership
- Catalogue compliance requirements
- Threat and risk assessments and reviews
- Risk management categorization
  - Criteria: confidentiality, integrity, availability

Security Integration/Ops

- ID standards, best practices, system specific requirements
- Determine controls needed
- Set performance metrics
  - Implementation
  - Efficiency
  - Effectiveness
  - Impact
- Set contingency and continuity plans

Security Integration/Ops -2

- Develop security plan
  - Business operations and strategic goals
  - Management goals and organization culture
  - Legal compliance
  - System architecture
- Develop policies
- Develop procedures

Policies

- Framework for decisions
- Elements
  - Internal policy
  - Compliance and monitoring discussion
  - Enforcement mechanism
- Levels
  - Organizational
  - Functional
  - Computing
  - Baseline

Procedures

- Take policies to day-to-day operations level
- “How-to”
- Detailed

Controls

- Evaluation criteria
- Provide basis for security assessment
- Description of item and statement of goal
- May be flexible

Implementation and Evaluation

- Hands on; documentation and security management software not enough
- Training
  - Vary by responsibilities
  - Mechanism to compel
- Test and evaluate
  - Implementation, efficiency, effectiveness, impact
- Identify weaknesses and have correction mechanism

Capital Planning & Investment Controls

- Make security part of processes
- ROI

Security Programs

Security Plan Norms

- Must be consistent with
  - Business operations
  - Legal compliance framework
  - Management goals
  - Organizational culture
  - Systems architecture

Security Plan Organization

- Boards of Directors
- Senior management
- Internal management
- Operational staff

Internal Management

- Business unit managers
- HR
- Legal
- Financial
- Technical
- Security
- PR

Assessment

- Includes Gap Analysis
- Analyze environment and assess risks and vulnerabilities
- Assess potential for problem
- Identify solutions or countermeasures
  - Appropriate and cost effective safeguards

Risk Assessment Strategies

- Avoid
- Mitigate
- Accept
- Transfer/Insure

IT Risk Managers

- Comparatively new concept
- Core of any approach, even if term not used
- Often taken from financial auditors and analysts

Common Flaws

- Failure to focus on value of information and business reputation
- Fix as little as possible and not follow up
- Assign untrained people and not give them instruction
- Ignoring problems
- Using surface solutions

Change Management

- Another relatively new concept
- Can help with many problems
- Systematic way to introduce and manage change
- Procedures for introducing and implementing
- Audit trail to trace problems back

Classification

- Gives framework for setting risk priorities
- Seems straightforward
  - Can be complicated
  - Often not done in systematic way
- Flexible process
- Must examine data life cycle
  - Create, access, use, modify, store
- Similar approach for applications and systems

Policies

- Components of plan
- Frameworks for decisions
- Place to add standards, guidelines, best practices
- Four levels
  - Corporate
  - Functional
  - Computing
  - Security baseline

Procedures

- Put into effect

Review

- At least annually for:
  - Effectiveness
  - Compliance
  - Vulnerability