

Computer Security

Security Policy

What is Security Policy?

- A set of rules/guidelines/definitions for the implementation and enforcement of security within an organisation
- Standards for use of IT resources

What does Security Policy Do?

- applies to **everyone**
- assigns responsibilities
 - What they should and should not do
- Establishes uniform procedures

Why Have a Security Policy?

- To ensure that security is applied to the organisations assets
- Without a comprehensive strategy there will be no comprehensive application of security
- There are too many risks to allow this to happen
 - Financial losses from computer crime are large and growing

Why?

- It's a part of normal risk-benefit analysis
- What would be the cost if a lack of computer security resulted in
 - Loss of information
 - unavailability of resources
- Lack of centralised security policy results in unfocussed, cohesive, security strategy

5

Note

- data handled by organisations varies in type and importance
- can't handle it all in the same way
- need some standardisation to avoid inconsistencies and risks
- So everybody knows what it is and what to do

6

Policy needs to be

- clear and comprehensive
- formulated in a way that will be accepted
- flexible

7

Policy Formulation

- requires input from many members of an organisation, not just the IT and/or security specialists
- under approval of senior management
- requires clear and unqualified support

8

Creating Policy

- Identify organisational assets
- Asses the risks
- Define the policy

Identify organisational assets

- Hardware
- Software
- Data
- People
- Documentation
- Supplies

Assessing the risk

- Identify possible attacks
 - From inside and outside
 - Unauthorised access
 - Unavailable service
 - Disclosure of information
 - Etc
- Evaluate the potential costs

Define the Policy - Questions

- who is allowed to use a resource?
- what is the proper use of a resource?
- who is authorised to grant access and approve usage?
- who may have sys admin privileges?
- what are users rights and responsibilities?
- rights and responsibilities of sys admin vs users?

Policy Document

- A policy document will consist of individual policy statements
- Each policy statement needs to be
 - Well considered
 - Well structured

Example Policy Statement Structure

- statement of issue
- statement of organisation's position
- applicability
- roles & responsibilities
- points of contact
- enforcement

Statement of Issue

- Statement about what the policy statement is addressing
- need clear definition
- relevant terms, distinctions and conditions
 - eg., “foreign software” - software (applications or data) not approved, purchased, screened, managed and owned by the organisation
 - distinctions for software owned and used by other organisations under contract

Statement of Organisation's Position

- This is the core of the policy
- must be clearly stated
- eg., foreign software, is it strictly prohibited?
- are there further guidelines for approval and use?
- or will case by case decisions be made on some defined criteria?

Applicability

- where, how, when, to whom, to what a policy applies
- eg., policy on foreign software applies to organisation's onsite resources and employees and not to contractor organisations with office at other locations

17

Roles & Responsibilities

- who does what
- if foreign software can be used at work with appropriate approval, who can give the approval?
- what are the penalties for using unapproved software on organisation's IT systems and who does the checking

18

Points of Contact

- appropriate individuals for further information, guidance, enforcement
- line manager? facility manager? tech support? sys admin? security specialist?
- who interprets the policy?
- individual or committee?
- who reviews and revises?

19

Enforcement

- need formal documented policy to be able to develop enforcement standards and mechanisms
- the penalties and disciplinary actions that can result from failure to comply with IT security requirements
- what results in firing? prosecution? written reprimand?

20

Policy Statement Scope

- high level
- low level

High Level Policy

- broad in scope
- establish the security framework
- assign management responsibilities
- state the organisation wide IT security goals and objectives
- provide a basis for enforcement

Low Level Policy

- issue specific
- identify and define specific areas of concern
- state organisations position and expectations in relation to such issues

Life time

- high level policy broad enough to not require much modification
- low level policy likely to require revision and updating
- technologies and related activities change
- issue increase and diminish in importance

High Level Policy - Purpose

- define
 - IT security management structure & reporting responsibilities
 - roles & responsibilities of individuals and groups
 - organisation wide goals
- emphasise
 - the importance of IT security
 - management support

25

High Level Policy - Scope

- includes all of organisations IT resources
- may name specific assets (major sites/large systems)
- includes overview of all types of IT resource (workstations, LANs, etc)

26

High Level Policy - Goals

- integrity, availability, confidentiality
- goals related to these concepts should be stated in **meaningful** ways
- should be relevant to employees based on the environment

27

Goals - Example

- large but not highly confidential database
 - goals specifically stressed include reduction in errors, data loss and data corruption
- confidential data
 - goals emphasise increased protection against unauthorised access and disclosure

28

High Level Policy - Responsibilities

- define management responsibilities
- responsibilities of line managers, application owners, data users, IT security personnel
- covers the activities and personnel integral to the implementation and continuity of IT security policy

29

High Level Policy - Responsibilities

- may define relationships between some individuals and groups
- eg., may specify who is responsible for approving the security measures for new systems or components (line manager of department or inter-departmental IT security specialist?)

30

High Level Policy - Training

- non-conformance can result from lack of knowledge or training
- or inadequate communication and explanation of policy
- high level policy needs to include orientation, training and realistic compliance timeframes

31

Low Level Policy

- address particular kinds of activities and, possibly, particular systems
- covers areas of current relevance, concern, controversy
- help to standardise activities
- provide guidelines for further development of procedures and practices

32

Example - E-mail

- who should have access to e-mail?
- how will access be assigned and monitored?
- for what types of activities and information is e-mail secure?
- how is forwarding handled?

33

Example - Virus threats

- exchange of floppy disks
- accessing bulletin boards
- use of shareware/freeware

34

More Examples

- resource consumption - what restrictions and who is restricted
- is account sharing permitted?
- how often should passwords be changed?
- restrictions on password formulation
- who is responsible for backups?
- policy on proprietary information
- statement on electronic mail privacy (is e-mail private to the user or owned by the organisation)?

35

Possible Areas for Security Policy

- physical security
- personnel security
- communications security
- administrative security
- risk management
- contingency planning

36

Physical Security

- physical protection of and access to IT resources
- who has access to what sites
- how often are risks analysed (and who does it)
- what physical access control/monitoring
- responsibilities of trained security
- responsibilities of everyone else

37

Personnel Security

- depends on activities performed and sensitivity of data
- develop and administer policies relating to screening, requirements, hiring, training, evaluating, firing
- who does it?

38

Communications Security

- complex
- use of cryptography, modems
- precautions to be taken against wiretapping
- e-mail, web use and other communication modes

39

Administrative Security

- input/output controls
- training and awareness
- security certification and awareness
- incident reporting
- configuration and change controls
- system documentation

40

Risk Management

- assess IT resources for threats and vulnerabilities
- plan means to counteract identified risks
- policies for how, by whom and when assessments made
- what type of documentation should result

41

Contingency Planning

- related to risk management
- planning for emergency actions to be taken
- which systems are most critical and therefore of highest priority
- how plans will be tested, how often, by whom
- who is responsible for approving plans?

42

Policy Implementation

- a process, not a pronouncement
- implementation only begins with formal issuance of policy

43

Policy Visibility

- security policy will affect all employees
- most resources of the organisation will be covered
- new terms and procedures will be introduced
- a new security policy is no minor event

44

Visibility

- can use
 - management presentations
 - panel discussions
 - guest speakers
 - forums
 - newsletters
 - IT security as a regular topic at staff meeting
- need unequivocal management support

45

Education

- organisation's security policy
 - Telling people what it is
 - And why we have it
- government regulations

46

Policy Documentation

- security policy must be included in organisation's formal documented policies
- this will probably involve both updating existing documentation and creating new documentation

47

Existing Documentation

- IT security will need to be included in existing activities and practices
- so will need to be included in their documentation
- documents, forms, plans at all levels may need to be revised

48

New Documentation

- many new documents required to support IT security policy
- guidelines, standards, procedure manuals, etc
- in large organisations may need to allow sub-units to tailor implementation to their needs

49

High Level vs Low Level

- high level
 - it is the policy of the organisation to ensure against data loss due to accidents or mishaps
- low level, area doing extensive word processing
 - policies on saving and use of auto-save
- low level, databases
 - policies on frequency of backups

50

Visibility

- IT security policy should be integrated in all relevant documents
- should be part of the daily routine

51

Possible Problems

- lack of planning or co-ordination (sub-units going their own way)
- lack of follow-up
- willingness to help (providing too much information, eg., passwords)
- unwillingness to follow procedure
- ego (I can do it myself)
- zeal (too much security)

52

Violation Response

- should be planned in advance
- actions based on kind of violation and kind of user

On Violation Discovery

- what outside agencies should be contacted?
- who should contact them?
- who may talk to the press?
- when are law enforcement agencies contacted?
- is remote site of origin contacted?
- What are the responsibilities to other Internet sites?

Possible Responses

- protect and proceed
- pursue and prosecute
- choice may be global or case by case
- policy must specify which and on what basis

Protect and Proceed

- primary goal is protection and preservation of resources
- attempts will be made to interfere with intruders progress
- immediate damage assessment and recovery
- if intruder not immediately identified they may attempt to re-enter

Protect and Proceed

- if assets not well protected
- if continued penetration poses great financial risk
- if unwilling to prosecute
- if user files vulnerable
- if users may sue if their resources compromised

Pursue and Prosecute

- allow intruders to continue unhindered until identified
- endorsed by law enforcement agencies
- if intruder internal may take disciplinary measures rather than legal - policy must specify

Pursue and Prosecute

- if system and resources well protected
- backups available
- risk of current intrusion outweighed by possible future attacks
- frequent attacks
- intruder access can be controlled
- pursuit possible

Pursue and Prosecute (cont)

- willingness to prosecute
- what evidence required is known
- organisation is prepared for legal action from users if their resources compromised