

# Developing Security Policies



## CSH5 Chapter 66 “Developing Security Policies” M. E. Kabay & Sean Kelley

1

Copyright © 2011 M. E. Kabay. All rights reserved.

## Topics

- Introduction
- Collaborating in Building Security Policies
- Phase I: Preliminary Evaluation
- Phase 2: Management Sensitization
- Phase 3: Needs Analysis
- Phase 4: Policies and Procedures
- Phase 5: Implementation
- Phase 6: Maintenance
- Some Resources for Policy Development
- Homework

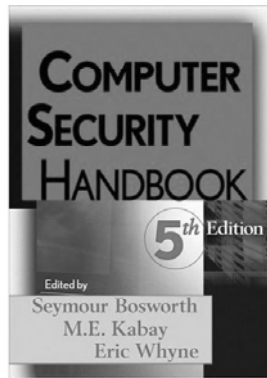


## Introduction



Many chapters in CSH5 deal explicitly with policy; e.g.,

- 22/23 – Physical Security
- 25 – LANS
- 44 – Guidelines
- 47 – OPSEC
- 45 – Employment
- 48 – E-mail / ‘Net Usage
- 49 – Awareness
- 50 – Social Psychology
- 52 – Application Controls
- 54 – Audits
- 56 – CSIRTs
- 57-59 – BU, BCP, DRP
- 66 – Developing Security Policies
- 67 – Developing Classification Policies



3

Copyright © 2011 M. E. Kabay. All rights reserved.

## Collaborating in Building Security Policies



- Organizational & individual resistance to policy development
  - ❑ Threats to self-perception, norms, habits, comfort, confidence
  - ❑ Fear of blame, interference, bureaucracy, delay
- Process of development influences acceptance
  - ❑ Must demonstrate personal benefits to all
  - ❑ Involve all parts of organization



Permission of © owners gratefully acknowledged.  
<http://tinyurl.com/2all5p>

4

Copyright © 2011 M. E. Kabay. All rights reserved.

## Phase I: Preliminary Evaluation



- Few organizations have policies that are
  - ❑ Complete
  - ❑ Maintained up-to-date
  - ❑ Understood
  - ❑ Monitored
  - ❑ Applied / enforced
- Must have formal authorization
  - ❑ Upper management support required
  - ❑ Even preliminary study needs explicit permission
    - ✓ Taking employee time and organizational resources



5

Copyright © 2011 M. E. Kabay. All rights reserved.

## Planning Evaluation



- Work Closely with HR Department
  - ❑ Must convince *department managers* to cooperate
  - ❑ HR staff likely to know key managers in each department
- Must design or use survey instruments
  - ❑ Questionnaires / surveys
  - ❑ Focus groups
  - ❑ One-on-one interviews
- Some HR staff may be experts in interview techniques
- May decide to use outside experts



6

Copyright © 2011 M. E. Kabay. All rights reserved.

## Preliminary Evaluation: Inventory



- Inventory precedes approval for full project
  - Only a few days of work
  - Ask everyone what *they perceive* as their most important security needs
- **NEVER argue or disagree with subjects!**
  - Job is to learn about issues from user perspective



7

Copyright © 2011 M. E. Kabay. All rights reserved.

## Preliminary Evaluation Checklist



- Introduce study – non-threatening
- State of current policy?
- Data classification?
- Sensitive systems?
- Critical systems?
- Authenticity issues?
- Exposure (consequences)?
- Responsibility and awareness?
- Physical security?
- Software development security?
- Computer operations security?
- Data Access Controls
- Network and communications security?
- Anti-malware measures?
- Backups, archives, data destruction?
- BCP / DRP?



Use audit checklists for more details

8

Copyright © 2011 M. E. Kabay. All rights reserved.

## Introduce Study – Non-Threatening



- Employees may perceive many questions as threatening
- Preamble or introduction should make clear
  - Not an audit
  - Not attempt to punish people
- Information should be anonymized
  - No person targeted for reprisal
- Reassure employees:
  - Study to learn about facts of security
  - Improvement
  - Not a search for culprits who will be punished

9

Copyright © 2011 M. E. Kabay. All rights reserved.

## State of Current Policy?



- Does enterprise have any security policies at all?
- Who developed them? Individual? Group?
- Where and how are security policies available (paper, electronic)?
- When were policies last updated? Last disseminated?
- Who, if anyone, has explicit responsibility for maintaining security policies?
- Who implements security policy at enterprise level?
- To whom does chief information security officer report within enterprise?
- Who monitors compliance with security policies, standards, and compliance?

10

Copyright © 2011 M. E. Kabay. All rights reserved.

## Data Classification?



- Levels of security classification that apply to your work? If so, what are they called?
- Are there rules for determining whether information you handle should be classified at a particular level of confidentiality?
- Are documents or files labeled to show their security classification?
- What is your opinion about value of such classification?
- Do people in your group pay attention to security classifications?
- Do you have any suggestions for improvement of how data are classified?

11

Copyright © 2011 M. E. Kabay. All rights reserved.

## Sensitive Systems?



- In your work, are there any kinds of information, documents, or systems that you feel should be protected against unauthorized disclosure? If so, name them.
- How do you personally protect sensitive information that you handle?
- How do others in your department deal with sensitive information? No names, please.
- To your knowledge, have there been any problems with release of sensitive information in your department?
- Do you have any suggestions for improving handling of sensitive data in your area?

12

Copyright © 2011 M. E. Kabay. All rights reserved.

## Critical Systems?



- In your work, are there any kinds of information, documents, or systems that you feel are so critical that they *must* be protected against unauthorized modification or destruction? If so, name them.
- Are there any special precautions you use or know of to safeguard critical data in your area?

13

Copyright © 2011 M. E. Kabay. All rights reserved.

## Authenticity Issues?



- Do you know of any cases in which anyone has used someone else's identity in sending out messages such as letters, faxes, or e-mail? If so, were there any consequences?
- Does anyone in your group use digital signatures on electronic documents?
- Does anyone in your group make or use unauthorized copies of proprietary software? If so, do you think there is any problem with that?

14

Copyright © 2011 M. E. Kabay. All rights reserved.

## Exposure (Consequences)?



- Worst consequences from publication of most sensitive information you control in newspapers?
- What if key competitors obtained specific confidential information that you use or control in your area?
- Monetary costs associated with scenarios you have described above?
- Worst consequences if critical information altered without authorization or through accidental modification?
- What if you could not access critical information quickly enough for your work?
- Estimate costs of such breaches of data integrity and data availability?
- What if someone forged documents in your name or in enterprise's name? Scenarios and associated costs resulting from such breaches of authenticity?

15

Copyright © 2011 M. E. Kabay. All rights reserved.

## Responsibility And Awareness?



- As far as you know, who is responsible for developing security policies?
- Do you know where to find the security policies that apply to your work?
- When, if ever, did you last sign any documents dealing with your agreement to security policies?
- Who is responsible for monitoring compliance with security policy in your work group? In the enterprise as a whole?
- Have you ever received any training in security policies? If so, when was the last time?
- Have you ever seen any written materials circulating in your work group that discuss information security?
- Do you think of protecting corporate information as one of your official responsibilities?

16

Copyright © 2011 M. E. Kabay. All rights reserved.

## Physical Security?



- Does anyone check your identity when you enter the building where you work?
- Are there any electronic access-control systems limiting access to your work area? What are they?
- Do people hold a secured door open to let each other into your work area? Do you let people in after you open a secured door?
- Have you ever seen a secured door into your area that has been blocked open (e.g., for deliveries)?
- Do people leave your work area unlocked when everyone leaves?

17

Copyright © 2011 M. E. Kabay. All rights reserved.

## Physical Security (cont'd)



- Do staff members wear identity badges at work? Are they supposed to? Do you wear your badge at work?
- Do visitors wear badges?
- Have you ever seen strangers in your area who are not wearing visitor badges?
- What would you do if you saw a stranger in your area who was not wearing a visitor's badge?
- Do you lock any parts of your desk when you leave your workspace?
- What would you do if you heard the fire alarm ring?
- Where is the nearest fire extinguisher?
- Who is the fire marshal for your floor?

18

Copyright © 2011 M. E. Kabay. All rights reserved.

## Physical Security (cont'd)



- What would you do if someone needed emergency medical attention?
- Is there an emergency medical station in your area or on your floor?
- Do you know who is qualified in cardiopulmonary resuscitation (CPR) in your group or on your floor? Do such people wear identifying pins?
- Have you had recent training in what to do in the event of an emergency? Have you been trained in how to evacuate the building?
- Is there anything that comes to mind that you would like to see to improve physical security and safety in your work area?

19

Copyright © 2011 M. E. Kabay. All rights reserved.

## Software Development Security?



- Are there any security policies that apply to your work? What are they?
- Have you ever discussed security policies in your group?
- Is security viewed positively, neutrally, or negatively in your group? And by yourself?
- Do you and your colleagues discuss security during the requirements analysis and specification phases when developing software?
- How do you see quality assurance as part of the development process?
- Do you use automated software testing tools?
- Tell us about version control in your group. Do you use automated version control software?

20

Copyright © 2011 M. E. Kabay. All rights reserved.

## SW Dev't Security (cont'd)



- How do you document your systems?
- Do you think that your source code is adequately protected against unauthorized disclosure and modification?
- What is your opinion about Easter eggs (unauthorized code for an amusing picture or game)?
- Could anyone plant an Easter egg or a logic bomb (unauthorized, harmful functions) in code being developed in your group?
- Have you ever seen an Easter egg or a logic bomb in code from your group? Did it get through to production?
- Can you think of ways you would like to see better security in your work?

21

Copyright © 2011 M. E. Kabay. All rights reserved.

## Computer Operations Security?



- How long do you wait after initial release before installing new operating system versions on your production machines?
- How do you put new software into production?
- Can development personnel access production software? Production data?
- How do you handle problem reports? Do you have an automated trouble-ticket system?
- Can people from outside the operations group enter the operations center?
- Are contractors, including repair technicians, allowed to circulate in operations without being accompanied?
- Do cleaning staff ever circulate within the secured areas of operations without operations staff present?

22

Copyright © 2011 M. E. Kabay. All rights reserved.

## OPSEC (cont'd)



- Are system components labeled?
- Is there an emergency cutoff switch for main power to the entire data center? Does it include air conditioning?
- Are there uninterruptible power supplies for critical components of your systems?
- Do you keep records of system downtime? What is your downtime over the last three months? The last year?
- What accounts for most of the downtime?
- Who monitors system resource utilization? Are there automated reports showing trends in disk space usage? CPU utilization? Network bandwidth usage?
- What improvements in security would you like to see in operations?

23

Copyright © 2011 M. E. Kabay. All rights reserved.

## Data Access Controls



- Do you have to identify yourself to the computers and networks you work with?
- Do you have a user name (ID) that no one else shares?
- Are you required to use a password, passphrase, or personal identification number (PIN) as part of your routine when starting to use your computer?
- Have you ever shared your unique user ID and password or PIN with someone else? Or have you borrowed someone else's user ID and password to get some work done? If so, how often does this happen?
- Do you use a token, such as a physical key or a smart card, to prove who you are to the computer system? If so, have you ever lent or borrowed such tokens? What for? How often?

24

Copyright © 2011 M. E. Kabay. All rights reserved.

## Data Access Controls (cont'd)



- In your work, are there any limitations on the data you are allowed to work with?
- Are there data you can see but not change?
- Do you use encryption on any of the data you work with?
- Do you or members of your group use laptop computers? If so, do you encrypt sensitive data on the disks of those portable systems?
- Do you or anyone in your group take work home? If so, do you put corporate data on your own, personal (noncompany) computers? Does anyone else have access to those computers? Are there any controls on accessing corporate data on the home computers?

25

Copyright © 2011 M. E. Kabay. All rights reserved.

## Network And Communications Security?



- As a user, do you know what the rules are about using your employer's e-mail system and Internet access?
- Do you know anyone who regularly violates system usage restrictions? No names, please.
- Have you ever seen pornography on corporate systems? Child pornography? Racist and other objectionable materials? If so, did you know what to do? And what did you do?
- Has anyone ever discussed rules for secure e-mail with you? Do you know how to encrypt sensitive messages? Do you ever encrypt messages?
- As a network manager, do you have up-to-date network diagrams, or can you produce them on demand?
- Do you know which services are running on your Internet-connected systems? Are all of the running services needed?

26

Copyright © 2011 M. E. Kabay. All rights reserved.

## COMSEC (cont'd)



- How do you determine which patches are appropriate for installation on your systems? How often do you check? Who is responsible for managing patches? How long does it take between notification of a vulnerability and installation of an appropriate patch?
- Does your security architecture include firewalls? If so, what determines the security policies you instantiate in the filtering rules?
- Do you have egress filtering enabled on your firewalls?
- Do you have intrusion detection systems? If so, who responds to apprehended intrusions? How are the responsible people notified of an intrusion?
- What are the procedures for responding to an intrusion?
- If your organization uses passwords, how do you handle requests for new passwords?
- Do you have centralized remote-access controls?
- Do remote users use virtual private networks (VPNs) to access corporate systems from outside the firewalls?

27

Copyright © 2011 M. E. Kabay. All rights reserved.

## COMSEC (cont'd)



- Are your users supposed to use encryption for sensitive e-mail that traverses the Internet? Do they? How do you know?
- Do your users apply digital signatures to all communications?
- Are your Web servers protected against intrusion and vandalism?
- Have you kept sensitive information off your Web servers?
- Do you encrypt all sensitive information stored on your Web servers?
- How long would it take you to recover a valid version of the Web site if it were destroyed or vandalized?
- Do your telephone voice-mail boxes have unique, nonstandard passwords? How do you know?
- How do you find out if an employee is being fired or has resigned? How long does it take between termination of employment of such an employee and deactivation of all system and network access?

28

Copyright © 2011 M. E. Kabay. All rights reserved.

## Anti-malware Measures?



- Do you and all of your users have antimalware products installed on every workstation?
- How often are antimalware products updated? How are they updated?
- How long does it take for all vulnerable systems to be brought up to date?
- Do you or your users open unexpected, unsolicited e-mail attachments?

29

Copyright © 2011 M. E. Kabay. All rights reserved.

## Backups, Archives, Data Destruction?



- How often do you do backups of your electronic data?
- Where do you store backup media? Are current copies retained off site as well as on? How do you know which media to use to restore a specific file?
- How long do you keep different types of backups? Why?
- How do you prevent unauthorized access to backup media?
- If you keep data backups for several years, how do you ensure that the old media will be readable and that the data developed for old applications will be usable?

30

Copyright © 2011 M. E. Kabay. All rights reserved.

## Backups (cont'd)



- How do you dispose of magnetic and optical storage media after their useful life is over? Are the discarded media readable?
- Do you make backup copies of paper documents? Where are these copies kept? How would you locate a specific document you needed?
- How long do you keep various types of papers? Why?
- When you dispose of paper documents, does their content influence how they are destroyed? How do you dispose of sensitive paper documents?

31

Copyright © 2011 M. E. Kabay. All rights reserved.

## BCP / DRP?



- Do you have business resumption planning (BRP) or disaster recovery plans (DRP)? If so, where are they kept?
- Who is responsible for keeping BRP and DRP up to date?
- Have you ever participated in a BRP or DRP testing? If so, how long ago was the last one? When is the next scheduled test?
- During BRP and DRP tests, does anyone use movie cameras or tape recorders to keep track of critical steps in the recovery?
- After a test, have you participated in analyzing the results of the tests to improve the plans?

32

Copyright © 2011 M. E. Kabay. All rights reserved.

## Phase 2: Management Sensitization



- Goal: approval for organization-wide audit & policy-formulation project
- Reason: upper management support *sine qua non*

### Tools

- Short meeting
- Sensitization videos
- Present results of preliminary survey
- Name working group
- Estimate time and costs
- Extra readings for managers



33

Copyright © 2011 M. E. Kabay. All rights reserved.

## Phase 3: Needs Analysis



- Information Protection Working Group (avoid "Security Group" – bad associations to name)
  - Reps from every sector of enterprise
  - Will provide important insights
  - Serve as ambassadors / cheerleaders / advocates within their own groups
- May need subcommittees if enterprise is large (>10,000 employees)



34

Copyright © 2011 M. E. Kabay. All rights reserved.

## Phase 4: Policies and Procedures



- Use existing templates as previously discussed (see next slide)
  - Avoid reinventing wheel
  - Usually see alternate versions of policies
  - Save months of work
- Ask for feedback from employees affected by policies
- Respond to legitimate needs

35

Copyright © 2011 M. E. Kabay. All rights reserved.

The screenshot shows a Microsoft Internet Explorer browser window. The address bar shows a file path: "File:///C:/My%20Documents/TSPME\_v10/Output/www/help/ja/html/frames.htm?context=TSPW". The page content includes a table of contents on the left and a main text area. The main text area is titled "Chapter 4 Sample High-Level Information Security Policy" and contains sections for "Role of Information And Information Systems", "Team Effort", "Involved Persons", and "Involved Systems".

## Phase 5: Implementation

- Use insights from social psychology (see Ch 50) to aid implementation
- Usually segment ATE (awareness, training and education) by sector and management level
  - ❑ Tailor presentations to audience
  - ❑ Provide most relevant policies and discussions



Copyright © 2011 M. E. Kabay. All rights reserved.

37

## Phase 6: Maintenance

- Continuing security-awareness programs
- UPDATE POLICIES to meet changing needs
- Annual rereading and signing of security agreement
- Monitoring and enforcement of policies



Permission of © owners requested.  
<http://tinyurl.com/22x484>

Copyright © 2011 M. E. Kabay. All rights reserved.

38

## Some Resources for Policy Development

### NOT an exhaustive list!

- ISPME
- NIST
- CERT-CC
- BSI
- SANS



Copyright © 2011 M. E. Kabay. All rights reserved.

39

## Information Security Policies Made Easy



Version 11

\$795

- Buy now!
- Buy two products and save \$195!
- Buy three products and save \$295!

- *Information Security Policies Made Easy, Version 11*
- Charles Cresson Wood
- <http://www.informationshield.com/ispmain.htm>

## NIST Special Publications

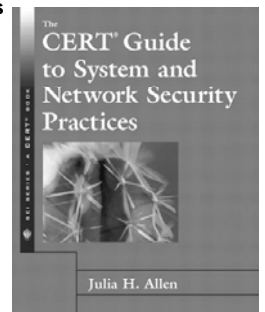
- Array of valuable documents – free! E.g.,
  - ❑ SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems (Feb 2007)
  - ❑ SP 800-41: Guidelines on Firewalls and Firewall Policy (Jan 2002)
  - ❑ SP 800-40 Version 2: Creating a Patch and Vulnerability Management Program (Nov 2005)
  - ❑ SP 800-41: Guidelines on Firewalls and Firewall Policy (Jan 2002)
  - ❑ SP 800-40 Version 2: Creating a Patch and Vulnerability Management Program (Nov 2005)
- <http://csrc.nist.gov/publications/nistpubs/index.html>

Copyright © 2011 M. E. Kabay. All rights reserved.

41

## CERT-CC

- Computer Emergency Response Team Coordination Center of SEI at CMU
- Valuable documentation (free) especially on CIRT-related matters
- <http://www.cert.org/index.html>
- CERT Security Improvement Modules <http://www.cert.org/security-improvement/>
  - ❑ Outsourcing Managed Security Services
  - ❑ Securing Desktop Workstations
  - ❑ Responding to Intrusions
  - ❑ Securing Network Servers
  - ❑ Deploying Firewalls
  - ❑ Securing Public Web Servers
  - ❑ Detecting Signs of Intrusion



Copyright © 2011 M. E. Kabay. All rights reserved.

42

## CERT-CC (cont'd)



- See also complete list of articles, reports and papers at <http://www.cert.org/nav/allpubs.html>
- Examples (of many)
  - ❑ *Advanced Information Assurance Handbook*
  - ❑ *CERT® System and Network Security Practices*
  - ❑ *Creating a Computer Security Incident Response Team: A Process for Getting Started*
  - ❑ *First Responders Guide to Computer Forensics*

43

Copyright © 2011 M. E. Kabay. All rights reserved.

## BSI



- IT-Grundschutz Manual = *Baseline IT Security*
- > 2000 pp of useful information in ENGLISH
- FREE in PDF
  - ❑ Introduction and Modules 2004 (7,2 MB)
  - ❑ Catalogues of Threats 2004 (2,6 MB)
  - ❑ Catalogues of Safeguards 2004 (22,6 MB)



[https://www.bsi.bund.de/cln\\_165/EN/Home/home\\_node.html](https://www.bsi.bund.de/cln_165/EN/Home/home_node.html)

44

Copyright © 2011 M. E. Kabay. All rights reserved.

## SANS Policy Resources



- SANS Security Policy Project
- <http://www.sans.org/resources/policies/>
- Community project with contributions from many organizations
- FREE materials
- List of topics follows on next slide

45

Copyright © 2011 M. E. Kabay. All rights reserved.

## SANS (cont'd)



- Acceptable Encryption Policy
- Acceptable Use Policy
- Analog/ISDN Line Policy
- Anti-Virus Process
- Application Service Provider Policy
- Application Service Provider Standards
- Acquisition Assessment Policy
- Audit Vulnerability Scanning Policy
- Automatically Forwarded Email Policy
- Database Credentials Coding Policy
- Dial-in Access Policyx
- DMZ Lab Security Policy
- E-mail Policy
- E-mail Retention
- Ethics Policy
- Extranet Policy
- Information Sensitivity Policy
- Internal Lab Security Policy
- Internet DMZ Equipment Policy
- Lab Anti-Virus Policy
- Password Protection Policy
- Remote Access Policy
- Risk Assessment Policy
- Router Security Policy
- Server Security Policy
- Third Party Network Connection Agreement
- VPN Security Policy
- Wireless Communication Policy

46

Copyright © 2011 M. E. Kabay. All rights reserved.

## Review Questions



1. Why does it matter how we develop and implement policies? Why not just impose them?
2. If you don't already have security policies in place, what's first step in trying to develop them? Why? I.e., why not just go ahead and develop them outright?
3. What kinds of push-back might you encounter in an organization as you try to create new security policies? Why? How can you overcome resistance?
4. As you plan your management-sensitization session, what would you look for in a training video?
5. Why would you segment employee population into different groups rather than just put everyone into a big auditorium and get it all over with in one go?
6. Why does maintenance involve changing policies? Shouldn't they be right from start?

47

Copyright © 2011 M. E. Kabay. All rights reserved.

# DISCUSSION



48

Copyright © 2011 M. E. Kabay. All rights reserved.