Isn’t it a chore writing security policies? Aren’t they just the most persnickety part of our job communicating security requirements to users? Whenever I teach human factors in information assurance, I emphasize the value of Charles Cresson Wood’s famous _Information Security Policies Made Easy_ (ISPME) to policy writers. I mentioned his work in one of my earliest columns for Networks World (<http://www.networkworld.com/newsletters/sec/2000/0717sec2.html>) back in 2000 and again in a column in 2001. (<http://www.networkworld.com/newsletters/sec/2001/00772793.html>) Charles Cresson Wood, CISSP, CISA, CISM is a distinguished contributor to our field; in addition to extensive consulting in a wide range of industries, publication of hundreds of professional articles and five books, and service as a professional editor, he has also contributed expert commentary to the public news media.<http://informationshield.com/aboutccw.htm>

Today I’m pleased to report on yet another fine contribution from Mr Wood: his _Information Security Roles & Responsibilities Made Easy_. (<http://informationshield.com/israr_main.htm>) Now in its second edition, this compendium provides a complement to the ISPME by providing what it claims – an extensive compilation of well-defined roles and responsibilities. The chapters are listed on a separate page. <link to a popup #1 containing the following text>

**CHAPTERS IN THE INFORMATION ROLES & RESPONSIBILITIES MADE EASY**

1: What This Book And CD-ROM Can Do For You
2: Reasons To Establish Clear R & R
3: Persuading Mgmt. To Document R and R
4: Before You Document R & R
5: Updating R & R
6: Who Should Write R & R Documents
7: Review & Approval Of R & R
8: Resources Required To Document R & R
9: Time Estimates To Document R & R
10: Key InfoSec Documents
11: Organizational Mission Statements
12: Job Descriptions For Specific Team Players
13: InfoSec Reporting Relationships
14: Template Customization Factors
15: Owner, Custodian, And User R
16: R & R Of Product Vendors
17: R & R Of Outsourcing Firms
18: Adjustments For Smaller Organizations
19: A Centralized Organizational Structure
20: Workers In InfoSec Related Positions Of Trust
21: Common Mistakes You Should Avoid
A: Staffing Levels
B: Personal Qualifications
Wood explains in his introduction (Chapter 1), “The entire process of developing and/or revising information security roles and responsibilities documentation has been scripted for you. The chapters in this book are deliberately sequenced so as to step you through all the important tasks on the road to developing professional, relevant, and effective information security roles and responsibilities documentation. The book provides you with all the detailed information you will need to prepare credible and meaningful memos to management to advance an information security roles and responsibilities project.”

An interesting point comes at the end of Chapter 2: “Perhaps the most significant reason to establish and document clear roles and responsibilities involves increasing worker productivity. Statistical studies of business economics indicate that about half of productivity growth over time comes from more efficient equipment, and about half comes from better trained, better educated, and better managed labor. Thus the clarification and publication of information security roles and responsibilities can have a substantial positive impact on productivity, and thereby markedly improve profits.” The chapter includes 35 other good reasons for establishing clear roles and responsibilities.

The text includes explicit discussions of how to communicate effectively with upper management; e.g., “With the intention to quickly obtain management approval, you should refrain from merging an information security roles and responsibilities project with any other project.” The next paragraph begins, “Beyond a memo, a brief meeting to discuss the project scope and the involvement of other groups is also recommended. At such a meeting, you can solicit management's ideas about all the different job titles and departments that in one way or another have something to do with information security. A good agenda for such a meeting would be:

1. Impediments to information security progress . . .
2. Benefits that come from clarifying information security roles & responsibilities . . .
3. Potential participants in an information security team . . .”

The text includes extensive provision for coordinating work with product vendors and with outsourcing services. Chapter 21 on “Common Mistakes You Should Avoid” has particularly useful insights that are explained in detail.
Mgmt. Has Not Been Sensitized To InfoSec Risks
No Executive Sponsor For InfoSec Has Been Arranged
Sufficient Mgmt. Approvals Were Not Obtained
Positioning Of InfoSec Conflicts With Organizational Objectives
Top Mgmt. Believes Its Duty Is Discharged By Appointing Someone
Accountability Does Not Match Responsibility
Staff Assumes Revenue Producing Activities Overshadow InfoSec
Mgmt. Says Everybody Is Responsible
Staff Takes A Reactive Approach To InfoSec
Mgmt. Relies On Voluntary InfoSec Cooperation
Contribution Made By InfoSec Is Not Regularly Reinforced
Mgmt. Does Not Reinforce New R And R
Major Projects Are Initiated Before R And R Are Defined
Scope Of InfoSec Duties Are Too Narrowly Defined
Scope Of InfoSec Duties Are Too Loosely Defined
Not Establishing Specific Enough Job Descriptions
Creating Job Descriptions Which Are Too Detailed
Inappropriate Person Prepares R And R Documents
Mgmt. Assigns Untrained And Inexperienced People
Mgmt. Is Unwilling To Pay Market Rates For Specialists
Technical Staff Inappropriately Promoted To Mgmt. Positions
Time Required To Get Top Mgmt. Approval Is Underestimated
R And R Are Not Periodically Updated
Staff Performance Reviews Do Not Include InfoSec
No Disciplinary Process Exists
No Compliance Checking Process Exists
No Clear Problem Reporting Process Exists

In summary, I think that as always, Charles Cresson Wood has come through with a thoughtful, helpful and well-organized resource for security policy implementation. Good on ya, Charles!

[DISCLAIMER: In case anyone has any suspicions, I have no financial interest whatever in the sale of Charles Cresson Wood’s texts. I just like them. A lot.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.