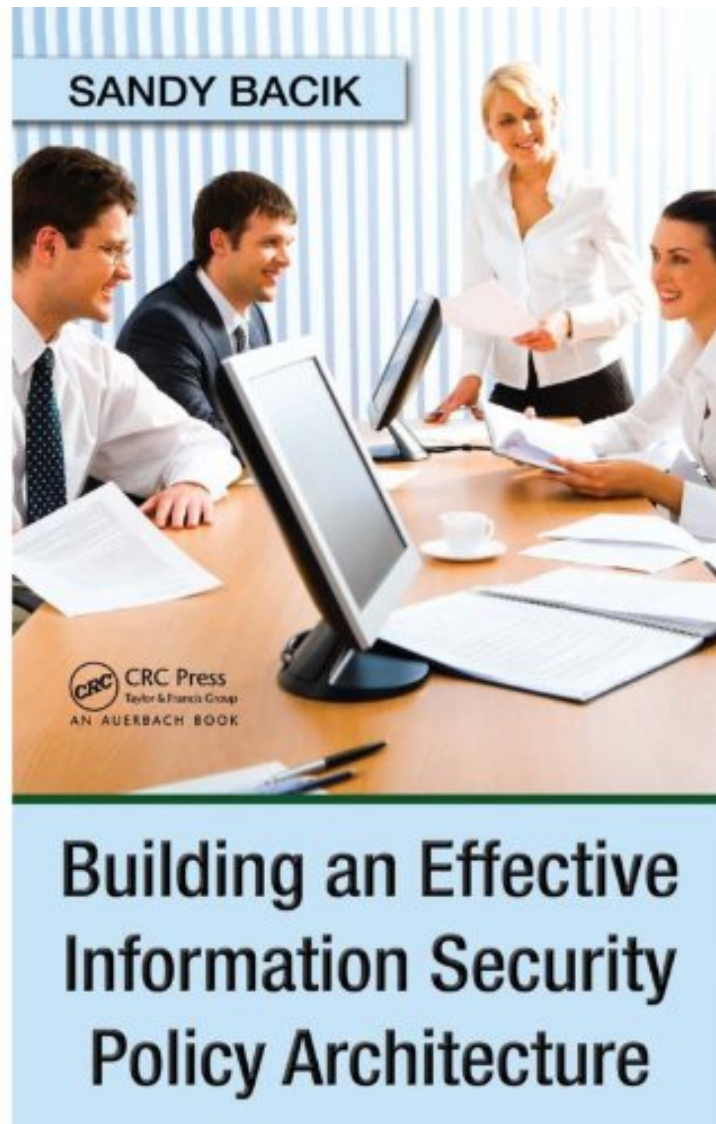


Building an Effective Information Security Policy Architecture

Sandy Bacik

*audiobook / *ebooks / Download PDF / ePub / DOC*



DOWNLOAD



READ ONLINE

#2012077 in eBooks 2008-05-20 2008-05-20 File Name: B008KZUO2Q | File size: 70.Mb

Sandy Bacik : Building an Effective Information Security Policy Architecture before purchasing it in order to gauge whether or not it would be worth my time, and all praised Building an Effective Information Security Policy Architecture:

4 of 4 people found the following review helpful. Does a good job of showing the reader how to start from scratch and build their security policy infrastructure By Ben Rothke Security policies are like fiber, that is, the kind you eat. Everyone agrees that fiber is good for you, but no one really wants to eat it. So too with information security policies. They are sorely needed, but most users don't go out of their way to comply with them. And in many firms, they are not even trained in what they have to do. But failure to have adequate information security policies can lead to myriad

risks for an organization. For the sake of a basic definition, a policy is a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. The purpose of information security is to protect an organization's resources. The cornerstone of any information security strategy is a robust set of policies, procedures, standards and guidelines. There are many reasons why information security policies are needed. Some of the most imperative reasons are:

- * To inform users of their information protection duties
- * Advise them what they can and cannot do with respect to sensitive information.
- * Define how users are permitted to represent the organization, what they may disclose publicly, and how they may use organizational computer resources for personal purposes.
- * To clearly define protective measures for these special information assets. The existence of a policy may be a decisive factor in a court of law, showing that the organization took steps to protect its intellectual property.
- * Define both acceptable and unacceptable behavior. For example, spending a lot of time surfing the web and downloading videos off the net are both generally unacceptable.
- * Policies are needed to establish the basis for disciplinary action, up to and including termination.

Building an Effective Information Security Policy Architecture does a good job of showing the reader how to start from scratch and build their security policy infrastructure. The book starts off at a high-level about the need for policies, and then goes into details on how to develop, write and sell these policies to management. The book is a good guide to the entire policy lifecycle, and how to use various means to get to the ultimate goal. At 340 pages, the first ten chapters comprise 155 pages and deal with creating the policy infrastructure, communicating with management, and putting the entire policy puzzle together. The final 185 pages comprise 21 appendices of various examples of different policies. A most significant downside and frustrating part to the book is that there is no CD-ROM with it, or companion website in which to download and use the numerous policy and process examples. At \$80.00, such an option should be de rigueur. The lack of electronic versions of the policies in a book such as this is senseless. Also, this is the first technology book that I have ever seen that did not cite a single reference. It is hard to imagine writing a book on this topic without using some sort of external reference. While the author may not want to quote sources, she should at least point the reader to other sources of information about security policies. Two notable and essential sources in the information security policy space are the SANS Institute - SANS Security Policy Project, which is free, and Information Security Policies Made Easy from Information Shield, Inc., which is \$795.00, but worth every penny for a serious security policy effort. Full disclosure: I am on the Information Shield Expert Panel, but get no financial incentives or compensation. Overall, Building an Effective Information Security Policy Architecture is a good resource to use if you are tasked to create or modify your organization's set of information security policies. The book will likely find itself on the desk of many information security professionals. While it is frustrating that the book makes you reinvent the wheel by not having electronic versions of the policies, its value still can't be underestimated. Let's hope future versions of the book will fix that anomaly.

1 of 1 people found the following review helpful. Building an Effective Information Security Policy Architecture by Sandy Bacik By Alexander Ivanov It is an easy-to-understand book that contains good advice, describes techniques how really to build a security policy, how to enable and maintain it within Your enterprise. To say the truth, this book helps to understand all the meal faster and better; this book is a real guide how to swim in Information Security pool. Alexander, IT administrator

Information security teams are charged with developing and maintaining a set of documents that will protect the assets of an enterprise from constant threats and risks. In order for these safeguards and controls to be effective, they must suit the particular business needs of the enterprise. A guide for security professionals, Building an Effective Information Security Policy Architecture explains how to review, develop, and implement a security architecture for any size enterprise, whether it is a global company or a SMB. Through the use of questionnaires and interviews, the book demonstrates how to evaluate an organization's culture and its ability to meet various security standards and requirements. Because the effectiveness of a policy is dependent on cooperation and compliance, the author also provides tips on how to communicate the policy and gain support for it. Suitable for any level of technical aptitude, this book serves as a guide for evaluating the business needs and risks of an enterprise and incorporating this information into an effective security policy architecture.