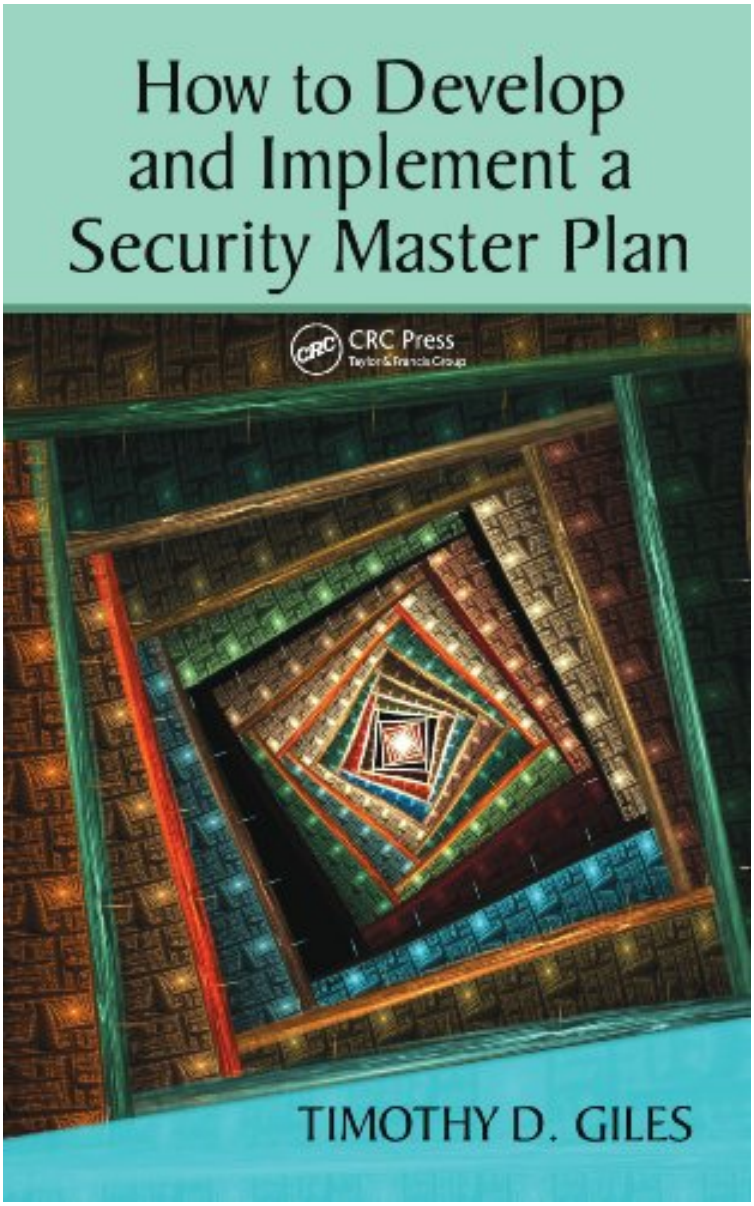
How to Develop and Implement a Security Master Plan

Timothy Giles
*ePub | *DOC | audiobook | ebooks | Download PDF*



#1665509 in eBooks 2008-12-17 2008-12-17File Name: B009AI8E2E | File size: 34.Mb

Timothy Giles : How to Develop and Implement a Security Master Plan before purchasing it in order to gage whether or not it would be worth my time, and all praised How to Develop and Implement a Security Master Plan:

0 of 0 people found the following review helpful. This book from cover to page 137 are blank. please advice on action .Adel KhedrBy Adel Khedr mahmoudThis book from cover to page 137 are blankPlease advice on actionAdel Khedr MahmoudAdel Khedr Mahmoud KAdelkhedr1@gmail.com0 of 0 people found the following review helpful. Review from the FieldBy Paul G. WellbornMr. Giles has taken decades of experience and knowledge and complied all that

any manager or director would need to develop an excellent master plan. I have reviewed Mr. Giles book and found it to be informative and a great tool for my own organizaion. The book will become part of an extensive list of recommended reading for all staff members. I have made it available to not only the security staff but property management as well. My thanks for Mr. Giles for making the next revision of my master plan much easier to improve.Paul G Wellborn, CPP9 of 11 people found the following review helpful. Master Plan - Don't BotherBy Ronald R. Baklarz Jr."How to Develop and Implement a Security Master Plan" by Timothy D. Giles CRC Press ISBN 978-1-4200-8625-6 2009 by Taylor Francis Group, LLCPurchased for a little over $70.00 with the intent that the content would assist in aspects of security planning and development, the book did not meet my expectations. To begin, I find the use of illustrations to be puzzling and inane. For example, Figure 1.2 depicts a lineup of faceless, suit-jacketed hands writing in notebooks as the writer apparently felt the need to describe `project teams'. For workplace violence, Figure 2.1 is a photograph of a mean-faced man shouting into a cell phone. Instead of supporting the content, these and other illustrations appear to be scattered throughout much like one would see in a bad Power Point presentation.Chapter 6 attempts to provide "Security and Computer Use Standards for Employees". The author advises users to activate power-on passwords for boot-up, hard disks access as well as encrypting files, etc. While these are certainly worthwhile goals, having a disparate user base responsible for setting and maintaining these features on their systems in any sizable organization is un-manageable even with IT department assistance. The chapter also discusses the evils of Napster file sharing. In a book as recent as this - 2009, there are a number of more heinous file sharing sites that should be referenced since Napster has now been legitimatized and deals primarily in music versus filesharing. And for some reason, the seemingly generic standards specifically identify that Norton anti-virus program be used. Overall, the information security section is lacking on many levels.Chapter 12 lays out the typical contents of a "security master plan." Interestingly, there is no mention of information security. All aspects of the master plan center around physical security including the "Security Technology Plan" section which touches on physical access control, CCTV, etc.While the physical security aspects of the book are somewhat better than the information security content, the overall criticism is that the book tries to cover too much area and never drills down deep enough in any one topic to be of any real value in developing security plans.Ron Baklarz CISSP, CISA, CISM, NSA-IAM/IEMJune 7, 2009

Engage Stakeholders with a Long-Term SolutionThe goal: Convince executive management to "buy in" to your security program, support it, and provide the largest possible amount of funding.The solution: Develop a meticulously detailed long-term plan that sells decision-makers on the dire need for your program, and then maps out its direction and required budget. Assess and Outline Security Risks to Map Out Mitigation Strategies This practical guide details how to construct a customized, comprehensive five-year corporate security plan that synchronizes with the strategies of any business or institution. The author explains how to develop a plan and implementation strategy that aligns with an organizationrsquo;s particular philosophies, strategies, goals, programs, and processes. Readers learn how to outline risks and then formulate appropriate mitigation strategies. This guide provides tested, real-world solutions on how to:Conduct an effective, efficient assessment of the site and security personnel, meticulously addressing the particular needs of many different environmentsMake decisions about security philosophies, strategies, contract relationships, technology, and equipment replacementInterview executive and security management to determine their concerns, educate them, and ensure that they buy in to your planUse all gathered data to construct and finalize the Security Master Plan and then implement it into the management of the businessApply Insights from an Expert with Global Experience at the Highest LevelAuthor Tim Giles worked at IBM for 31 years serving as Director of Security for the companyrsquo;s operations in the United States and Canada, as well as Latin America and Asia-Pacific. His immeasurable experience and insight provide readers with an extraordinarily comprehensive understanding that they can use to design and execute a highly effective, tailored security program.

This practical guide details how to construct a customized, comprehensive, five-year corporate security plan that synchronizes with the strategies of any business or institution.ndash; In ASIS Dynamics, May/June 2009 In this well-written, well-organized book, author Timothy D. Giles, CPP, PSP, provides a thorough overview of how to develop a five-year security master plan that aligns with both an organizationrsquo;s security philosophy and its overall business plan. hellip; In addition to explanation of data collection and analysis procedures, the text features an outline of a plan document including guidelines for how to address the budget and establishing a return on investment, as well as a discussion on how to approach the final recommendationsrsquo; presentation. hellip; A valuable appendix includes guidelines for dealing with workplace violence issues, material on executive protection, self-assessment templates, and an example of a format for a consulting proposal. hellip; It is an excellent road map for security professionals to use as a benchmark relative to their own practices and would also be an excellent text for students assigned to evaluate a security program.?George Okaty, Director of Safety Security, Tidewater Community College, Virginia, in Security Magazine, September 2010