THE EXPERT'S VOICE® IN CYBERSECURITY

Enterprise Cybersecurity Study Guide

How to Build a Successful Cyberdefense Program Against Advanced Threats

Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam

Apress®

Enterprise Cybersecurity Study Guide

How to Build a Successful Cyberdefense Program Against Advanced Threats

Scott E. Donaldson
Stanley G. Siegel
Chris K. Williams
Abdul Aslam

Apress®

Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats

Scott E. Donaldson
Falls Church, Virginia, USA

Stanley G. Siegel
Potomac, Maryland, USA

Chris K. Williams
San Diego, California, USA

Abdul Aslam
San Diego, California, USA

ISBN-13 (pbk): 978-1-4842-3257-6
ISBN-13 (electronic): 978-1-4842-3258-3
https://doi.org/10.1007/978-1-4842-3258-3

Library of Congress Control Number: 2018935923

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Todd Green
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484232576. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

To my growing family: Shelly, Ashleigh, Melanie, Manoli, Nick, Stephanie, David, Jackson, Mason, Julia, Laura, and Justin

—Scott Donaldson

To Bena, my wife, and our grandchildren: Eva, Ezra, Avi, Raffi, Tal, Eli, Zoe, Sarah, Emma, and Simcha

—Stan Siegel

To my father, Dennis, who taught me to protect those whom you love, and love those whom you protect

—Chris Williams

To my parents: Zahida, Maqbool, Shamim, and Imam. And to my loves: Sharu, Ishaq, Farhan, and Zayd

—Abdul Aslam

Contents at a Glance

Contents

About the Authors

Scott E. Donaldson's professional experience includes working in federal, commercial, and university marketplaces as well as in the defense industry. His expertise includes multimillion-dollar program management, systems development, information technology, business operations, business development, and technology cultural change. He has served in a wide variety of leadership roles including Chief Technology Officer (CTO), IT Director, Chief Systems Engineer (CSE), Program Manager, Line Manager, and Business Development Capture Manager. He has developed new technologies, techniques, and practices to bring in new business by solving real-world problems.

Donaldson teaches software engineering, software process improvement, and information management courses at the Johns Hopkins University's Whiting School of Engineering. Johns Hopkins honored him in 2009 with an Excellence in Teaching Award. He has a BS in Operations Research from the United States Naval Academy and a MS in Systems Management from the University of Southern California.

Donaldson has co-authored three software engineering books: *Successful Software Development: Making It Happen, 2nd Edition* (Prentice Hall PTR, 2001); *Successful Software Development: Study Guide* (Prentice Hall PTR, 2001); and *Cultivating Successful Software Development: A Practitioner's View* (Prentice Hall PTR, 1997).

Donaldson has contributed to other software engineering books, including the *Encyclopedia of Software Engineering: Project Management—Success Factors* (CRC Press, 2010) and the *Handbook of Software Quality Assurance: Software Configuration Management—A Practical Look, 3rd Edition* (Prentice Hall, 1999).

Donaldson also co-authored *CTOs at Work* (Apress, 2012) and *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (Apress, 2015).

Dr. Stanley Siegel has progressive professional experience as a systems engineer, mathematician, and computer specialist. He holds a nuclear physics doctorate from Rutgers University. He started his career with the US government in the Department of Commerce and then the Department of Defense. After his government service, he worked with Grumman for 15 years and Science Applications International Corporation (SAIC) for over 20 years. He helped SAIC grow to an 11-billion-dollar leader in scientific, engineering, and technical solutions with hundreds of millions of dollars in new business.

While at SAIC, he served as a senior technical advisor and director on a wide spectrum of projects in areas such as software engineering methodology assessment, software requirements analysis, software testing and quality assurance, and technology assessment.

In the 1990s, Siegel and Donaldson developed the Object Measurement Methodology, which appears in *Enterprise Cybersecurity*. This methodology can be used to quantify an enterprise's cybersecurity effectiveness in warding off cyberattacks. As the book explains, the enterprise can improve its cyberdefenses by taking corrective actions by using this methodology.

Siegel and Donaldson have jointly taught graduate courses since the mid-1990s. They teach both in-class and online software systems engineering courses at Johns Hopkins University's Whiting School of Engineering. Johns Hopkins honored them both in 2009 with an Excellence in Teaching Award.

Siegel has co-authored four software engineering books including the seminal software engineering textbook *Software Configuration Management: An Investment in Product Integrity* (Prentice Hall, 1980). He has contributed to a number of books, including the *Encyclopedia of Software Engineering: Project Management—Success Factors* (CRC Press, 2010) and the *Handbook of Software Quality Assurance: Software Configuration Management—A Practical Look, 3rd Edition* (Prentice Hall, 1999).

Chris Williams has been involved in the cybersecurity field since 1994. He has held both US military and commercial positions. He has been with Leidos (formerly SAIC) since 2003, focusing on enterprise cybersecurity and compliance. Previously, he worked with EDS (now HP) and Booz Allen Hamilton. He is a veteran of the US Army, having served five years with the 82nd Airborne Division and 35th Signal Brigade. He has worked on cybersecurity projects with the US Army, Defense Information Systems Agency, Department of State, Defense Intelligence Agency, and numerous other commercial and government organizations, designing integrated solutions to protect against modern threats. Williams holds a BSE in Computer Science Engineering from Princeton University and a MS in Information Assurance from George Washington University.

Williams co-authored *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (Apress, 2015). He holds a patent for e-commerce technology and has published technical papers with the Institute of Electrical and Electronics Engineers (IEEE). He has presented on cybersecurity at RSA, Milcom, the International Information Systems Security Certification Consortium (ISC), the Information Systems Security Association (ISSA), and other forums.

Abdul Aslam has over 20 years of experience in devising risk acceptance and compliance frameworks, application security, security operations, and information protection. He is the Director of Cyber Security Audit for Leidos tasked to evolve and maintain the corporate Cyber Security assessment and audit program. He was the Director of Cyber Security Governance, Risk, and Compliance for Leidos where he was in charge of delivering secure and scalable security solutions, policy governance, and strategic technology support. He has worked on numerous IT projects with a proven record of pioneering innovative systems analysis processes and secure application designs that improve availability, integrity, confidentiality, reliability, effectiveness, and efficiency of technology services.

Aslam has a MS in Systems Engineering Management and Information Assurance from the George Washington University and a BS in Engineering in Electronics and Telecommunications from Osmania University (India). He also has CISSP certification.

Aslam co-authored *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (Apress, 2015) and has presented on cybersecurity at International Information Systems Security Certification Consortium (ISC)^2 and the Information Systems Security Association (ISSA).

About this Study Guide

Preface

This study guide is an instructional companion to the book *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*. This study guide increases students' understanding of the book's ideas, whether they are using it in the classroom or for self-study. The study guide is structured to be self-explanatory and is intended to augment the book's content. For additional information and detail on the topics covered in this study guide, please reference *Enterprise Security: How to Build a Successful Cyberdefense Program Against Advanced Threats* by Scott E. Donaldson, Stanley G. Siegel, Chris Williams, and Abdul Aslam (Apress, 2015) (www.apress.com/9781430260820).

Implementing a successful cyberdefense program against real-world attacks is what *Enterprise Cybersecurity* is about. Often in cybersecurity, everyone knows *what should be done*, but resources *to do it* are not sufficient. Organizations must prioritize their efforts to deploy an incomplete solution that they "hope" is sufficient. The challenge lies in how to prioritize resources so security can be as successful as possible. As shown in Figure P-1, the Cybersecurity Conundrum often gets in the way of what needs to be done, leaving gaps in enterprise cyberdefenses that are exploited by clever attackers.

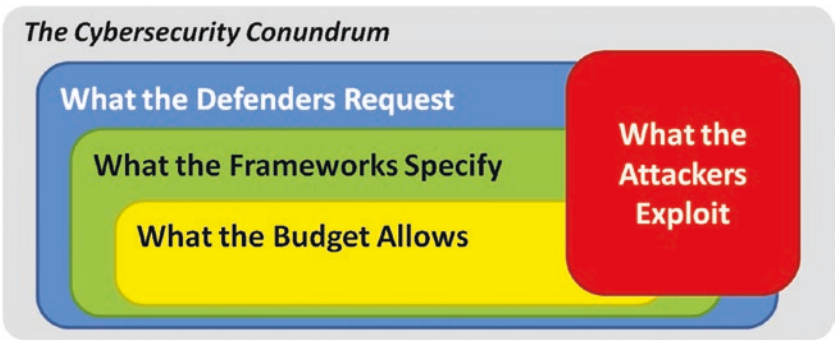

Figure P-1. *Even though the cybersecurity conundrum presents significant challenges, implementing a successful cyberdefense program that works against real-world attacks is achievable.*

One Cybersecurity Conundrum challenge is that cybersecurity professionals want to implement more than what control frameworks specify and much more than what the budget allows. Ironically, another challenge occurs even when defenders get everything that they want; clever attackers are extremely effective at finding and exploiting the gaps in defenses, regardless of their comprehensiveness. The overall challenge, then, is to spend the available budget on the right protections so that real-world attacks can be thwarted without breaking the bank and that they also comply with mandated regulatory requirements.

Intended Audiences

As shown in Figure P-2, people involved in or interested in successful enterprise cybersecurity can use this study guide to gain insight into an effective architecture for coordinating an entire cyberdefense program.

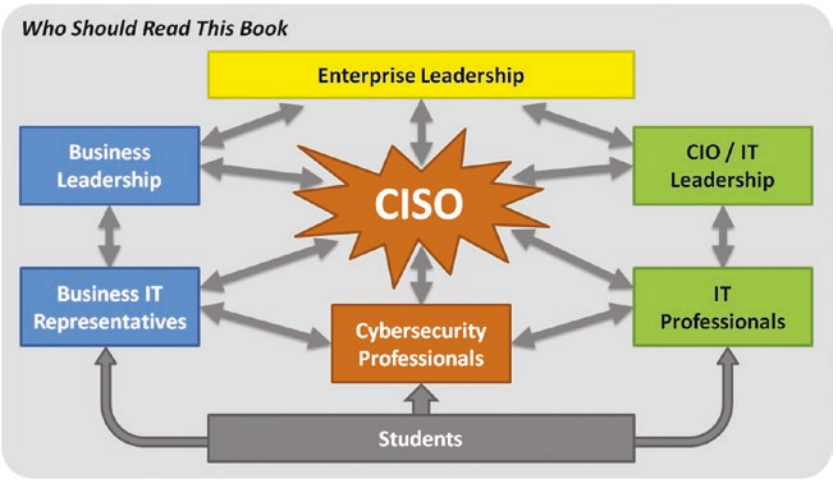

Figure P-2. *Successful enterprise cybersecurity is a team sport.*

This study guide is intended for the following audiences:

- **Everyone involved in or interested in successful enterprise cybersecurity**. This study guide offers material for those who want to use the book to help them do their work. Such individuals can use this material to learn about cybersecurity and its challenges, cybersecurity implementation, effective cyberdefenses, pragmatic cyberincident response, cybersecurity program assessments, and cybersecurity program management. In short, this study guide helps those who need to understand the challenges of delivering effective cybersecurity solutions.
- **Students**. This study guide recasts the book's contents as presentation material. This material is organized according to the chapter organization of the original book, with major points appearing generally in the same order as they appear in the book. Most of the book's figures, or adaptations of these figures, appear in this study guide. Students can use this material in a number of ways in conjunction with the text to include the following examples:
  - Before reading a chapter or part of a chapter from the book, students can go to the corresponding study guide pages to get a quick look at the chapter or chapter part and understand its major points and themes.
  - While reading a chapter or chapter part, students can, in parallel, look at the corresponding study guide pages. Sometimes a different look at the same material can facilitate learning.
  - After reading a chapter or chapter part, students can go to the corresponding study guide pages to quickly review key points, concepts, and descriptive figures.

- **Instructors**. This study guide offers material that instructors can use to develop classroom presentations based on the book's contents. Instructors can also use these pages to incorporate material from the book into other courses. For example, an instructor may be teaching a course (or part of a course) on the topic of cybersecurity assessments. If such a course is presenting different approaches to cybersecurity assessments, "Chapter 11: Assessing Enterprise Cybersecurity" and/or "Appendix D: Cybersecurity Sample Assessment" in this study guide may offer the instructor ready-made material for demonstrating one example of a comprehensive assessment methodology.

Using Study Guide Material

This study guide material can be used in a number of ways that include the following:

- **Corporate Education**. This material can be used to teach a short course to employees within an organization or to teach a more detailed course targeted at cybersecurity professionals. The course can address all the book's material or selected material for special topics.
- **University Education**. This material is suitable for a course at the undergraduate and graduate levels. The material can be covered quickly in a single overview course, or it can be covered in more detail as part of a larger cybersecurity instruction program. When considered in depth, the material of this study guide may be too extensive to be thoroughly covered in a one-semester, three-credit course.

  This guide can be used to structure short presentations on selected topics from the book. In the university environment, this approach can be used to structure a graduate-level special topics seminar spanning multiple weeks, and perhaps meeting for a couple of hours each week to discuss detailed topics drawn from the book and other industry literature. Such a seminar might be used to help students conduct their own research and assess other information sources from books, literature, and the Internet.
- **Professional Conferences and Meetings.** The authors offer the following suggestions to those involved with establishing cybersecurity training programs:
  - This material can be used to give presentations at professional conferences and other meetings pertaining to cybersecurity (such as the Information Systems Security Association [ISSA]).
  - This material can be used to structure short presentations (say, one hour) to introduce employees to key cybersecurity-related topics such as common cybersecurity attacks, cybersecurity frameworks, cybersecurity policy, and cybersecurity operational processes.
  - This material can be used to structure half-day or longer presentations dealing with the how-tos of such topics as cybersecurity assessments audits and measuring a cybersecurity program.

- The material can be used to augment existing training activities:
  - The material found in "Appendix C: Object Measurement" can be added to an existing presentation on measurement. One purpose of such an addition would be to illustrate alternative ways of addressing the challenging problem of meaningful cybersecurity measurement.
  - This material can be added to a new module as a self-contained presentation. For example, a company may have one or more training modules dealing with different aspects of the business case for cybersecurity improvement. This material could be included in a module that focuses on return on investment, while another module might focus on cybersecurity effectiveness.

How This Study Guide Is Organized

- ***Introduction***
  The introduction lays the groundwork for subsequent discussions on how to start, continue, and improve an enterprise's cybersecurity. This section provides an introductory understanding of cybersecurity and explains how cybersecurity is with us to stay.
- ***Part I: The Cybersecurity Challenge***
  Part I is about the cybersecurity challenge and how cybersecurity has changed over the past decade. Due to this evolution, the cyberdefense methods that worked well in the past are doomed to fail in the future.
  - *Chapter 1: Defining the Cybersecurity Challenge*
    This chapter defines the cybersecurity challenge facing the modern enterprise and discusses the threats against its defenses and why those threats are succeeding at an alarming rate.
  - *Chapter 2: Meeting the Cybersecurity Challenge*
    This chapter describes how the cybersecurity challenge can be met and how cybersecurity controls and capabilities can be organized to prevent, detect, document, or audit malicious behavior.
- ***Part II: A New Enterprise Cybersecurity Architecture***
  Part II introduces a new enterprise cybersecurity architecture that is designed to organize and manage every aspect of an enterprise cybersecurity program, including policy, programmatics, IT life cycle, and assessment.
  - *Chapter 3: Enterprise Cybersecurity Architecture*
    This chapter describes the new enterprise cybersecurity architecture and explores 17 functional areas in terms of their goals and objectives, threat vectors, and underlying capabilities.
  - *Chapter 4: Implementing Enterprise Cybersecurity*
    This chapter discusses how to implement the new enterprise cybersecurity architecture by identifying security scopes, defining security policies, and selecting security controls to counter anticipated threats.

- *Chapter 5: Operating Enterprise Cybersecurity*
  This chapter explains how to operate enterprise cybersecurity capabilities and processes, including 17 operational processes and 14 supporting information systems essential to effective enterprise cybersecurity.
- *Chapter 6: Enterprise Cybersecurity and the Cloud*
  This chapter discusses how cloud computing is different from the conventional data center and explains how the new architecture needs to be tailored for cloud computing environments.
- *Chapter 7: Enterprise Cybersecurity for Mobile and BYOD*
  This chapter describes the trends of mobile computing and Bring Your Own Devices (BYODs) and how these two trends solve problems and introduce challenges for the new architecture.

- ***Part III: The Art of Cyberdefense***
  Part III discusses the art of cyberdefense and how the new architecture is deployed and used to provide effective risk mitigation and incident response for cybersecurity crises.
  - *Chapter 8: Building an Effective Defense*
    This chapter examines why attackers have great success against legacy cyberdefenses, how the steps of the attack are sequenced and how to disrupt them, and how to layer cyberdefenses so they effectively thwart targeted attacks.
  - *Chapter 9: Responding to Incidents*
    This chapter describes the incident response process in detail by considering what the enterprise needs to do on an ongoing basis to investigate, contain, and remediate cybersecurity incidents when they occur.
  - *Chapter 10: Managing a Cybersecurity Crisis*
    This chapter discusses how severe cybersecurity incidents become crises and how the enterprise must behave differently in a crisis situation while it struggles to restore normal operations.
- ***Part IV: Enterprise Cyberdefense Assessment***
  Part IV establishes a methodology for quantitatively and objectively assessing cybersecurity using the enterprise cybersecurity architecture and then mapping those assessments against major frameworks for reporting purposes.
  - *Chapter 11: Assessing Enterprise Cybersecurity*
    This chapter explains the cybersecurity assessment and auditing process, and provides four worked-out examples using the new architecture to assess cybersecurity posture and effectiveness.
  - *Chapter 12: Measuring a Cybersecurity Program*
    This chapter provides a comprehensive method for objectively measuring an enterprise's cybersecurity by looking at risk mitigations, cybersecurity functional areas, and security operations.
  - *Chapter 13: Mapping Against Cybersecurity Frameworks*
    This chapter explains how to take the results of an enterprise cybersecurity assessment and map them against other cybersecurity frameworks for the purpose of evaluation, audit, or compliance reporting.

- ***Part V: Enterprise Cybersecurity Program***
  Part V brings together the concepts of the rest of the book into a comprehensive enterprise cybersecurity program that combines assessment, planning, prioritization, implementation, and operations.
  - *Chapter 14: Managing an Enterprise Cybersecurity Program*
    This chapter explains the cybersecurity program management process and shows how the enterprise can use it to manage cybersecurity decision-making and prioritize improvements to get the best possible value for the investment.
  - *Chapter 15: Looking to the Future*
    This chapter concludes the study guide by discussing the evolution of generations of cyberattacks and cyberdefenses, and how enterprise cybersecurity architecture will evolve over time to support the enterprise's needs now and in the future.
- ***Part VI: Appendices***
  The appendices provide greater detail than the chapters and provide important details and examples for cybersecurity practitioners who want to use the enterprise cybersecurity architecture described in this study guide.
  - *Appendix A: Sample Cybersecurity Policy*
    This appendix provides a sample enterprise information security policy document, organized into the 11 functional areas of the new architecture described in this study guide.
  - *Appendix B: Cybersecurity Operational Processes*
    This appendix contains detailed flowcharts for the 17 operational processes of enterprise cybersecurity, and it also introduces the 14 supporting information systems.
  - *Appendix C: Object Measurement*
    This appendix introduces the Object Measurement Methodology for objective assessment and explains how to use it to measure and report enterprise cybersecurity architecture effectiveness.
  - *Appendix D: Cybersecurity Sample Assessment*
    This appendix provides an example enterprise cybersecurity assessment using the methodology contained in this study guide, providing multiple levels of details showing how different types of assessment can be performed.
  - *Appendix E: Cybersecurity Capability Value Scales*
    This appendix contains detailed, example Object Measurement value scales for measuring the performance of each of the 113 enterprise cybersecurity architecture capabilities, grouped by the 11 functional areas.

Summary

- This study guide is an instructional companion to the book *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*.
- This study guide contains landscape-formatted pages that recast the book's content and new content as presentation material.
- This material is organized according to the chapter structure of the original book and is laid out in the order that it appears in each chapter.
- This study guide is intended for everyone involved in or interested in successful enterprise cybersecurity (business professionals, IT professionals, cybersecurity professionals, students, and so on).
- Students, cybersecurity professionals, and IT professionals can use this study guide in a self-study manner. Students can also use this study guide to facilitate note-taking in the classroom.
- Instructors can use this study guide to develop classroom presentations based on the book's contents.
- This study guide, in conjunction with the book, can be used by anyone who wants to learn and apply what it takes to build a successful cyberdefense program against advanced threats.