Michael Gregg and Billy Haines

CASP

CompTIA® Advanced Security Practitioner

STUDY GUIDE

CompTIA
ADVANCED SECURITY PRACTITIONER
CASP

CompTIA AUTHORIZED

EXAM CAS-001

Includes Real-World Scenarios, Lab Exercises, and Access to Exam Prep Software Featuring:

+ Custom Test Engine
+ Hundreds of Practice Questions
+ Electronic Flashcards

CompTIA AUTHORIZED PARTNER GOLD

SYBEX SERIOUS SKILLS.

CASP

CompTIA® Advanced Security Practitioner

Study Guide

CASP

CompTIA® Advanced Security Practitioner

Study Guide

Michael Gregg

Billy Haines

WILEY

John Wiley & Sons, Inc.

Senior Acquisitions Editor: Jeff Kellum
Development Editor: Dick Margulis
Technical Editors: Shawn Merdinger and Billy Haines
Production Editor: Eric Charbonneau
Copy Editor: Liz Welch
Editorial Manager: Pete Gaughan
Production Manager: Tim Tate
Vice President and Executive Group Publisher: Richard Swadley
Vice President and Publisher: Neil Edde
Media Project Manager 1: Laura Moss-Hollister
Media Associate Producer: Josh Frank
Media Quality Assurance: Marilyn Hummel
Book Designer: Judy Fung
Compositor: Craig Woods, Happenstance Type-O-Rama
Proofreader: Jen Larsen, Word One New York
Indexer: Ted Laux
Project Coordinator, Cover: Katherine Crocker
Cover Designer: Ryan Sneed

Published simultaneously in Canada

ISBN: 978-1-118-08319-2 (pbk)

ISBN: 978-1-118-22272-0 (ebk)

ISBN: 978-1-118-23661-1 (ebk)

ISBN: 978-1-118-26152-1 (ebk)

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Not all content that is available in standard print versions of this book may appear or be packaged in all book formats. If you have purchased a version of this book that did not include media that is referenced by or accompanies a standard print version, you may request this media by visiting `http://booksupport.wiley.com`. For more information about Wiley products, visit us at `www.wiley.com`.

Library of Congress Control Number: 2011945563

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *CASP: CompTIA Advanced Security Practitioner Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at `nedde@wiley.com`. If you think you've found a technical error in this book, please visit `http://sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,

Neil Edde
Vice President and Publisher
Sybex, an Imprint of Wiley

To Christine, thank you for your love and for always supporting me in my endeavors.
I love you.
—Michael Gregg

I would like to dedicate this, my first book, to God, my beloved wife Jackie, my son John, my parents and grandparents Bill and Jeannette and Bill and Bettie respectively, and finally to my Uncle Cliff.
—Billy Haines

Acknowledgments

I want to acknowledge and thank the talented team at Sybex and Wiley for their tireless pursuit of accuracy, precision, and clarity. Thank you for your skillful efforts.

I would also like to acknowledge and thank you, the reader, for your desire for self-improvement and your faith in us to produce a resource worthy of your time, money, and consumption. We've done our best to make this a powerful asset in your efforts to be a better IT professional. To all of you who read this book, keep learning and taking steps to move your career forward.

—*Michael Gregg*

First I would like to acknowledge the Sybex team—Pete, Jeff, Liz, and Eric; Michael Gregg for giving me the opportunity; Mary Purdy with BAH for pushing ever-so-gently in the direction of the CASP; my Warrant CWO3 Walter Moss for pushing me not-so-gently in every other direction; my Commanding Officer CDR Matthew Rick for his recognition and sheer patriotism; Adam Liss of Google for recommending the Google Authors conference among many other things; and finally Rickey Jackson for his BackTrack support and externally facing X-Windows: no, I will never let you live that one down.

—*Billy Haines*

About the Authors

Michael Gregg is the founder and president of Superior Solutions, Inc., a Houston, Texas–based IT security consulting firm. Superior Solutions performs security assessments and penetration testing for Fortune 1000 firms. The company has performed security assessments for private, public, and governmental agencies. Its Houston-based team travels the United States to assess, audit, and provide training services.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating emerging technologies. He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to co-writing the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or co-written 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (ISBN: 978-0470179864), *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (ISBN: 978-1597491099), *Certified Ethical Hacker Exam Prep 2* (ISBN: 978-0789735317), and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (ISBN: 978-0672328091).

Michael has created over a dozen training security classes and training manuals and is the author of the only officially approved third-party Certified Ethical Hacker training material. He has created and performed video instruction on many security topics such as Cyber Security, CISSP, CISA, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and giving back to the community. He is a board member for Habitat for Humanity.

Billy Haines is a computer hobbyist/security enthusiast. He served six years in the United States Navy and has visited 19 countries. He currently possesses various certifications, including the CCNA Security and CISSP Associate. His home lab consists of a variety of Cisco equipment ranging from 1841 routers to 3550 and 3560 switches. He runs a myriad of operating systems, including Debian Linux and OpenBSD, and has served as the technical editor for a variety of security-related publications. He can be reached at `billy.haines@hushmail.com`.

Contents at a Glance

Contents

Table of Exercises

Foreword

Qualify for Jobs, Promotions, and Increased Compensation

CompTIA CASP is an international, vendor-neutral certification that helps ensure competency in:

- Enterprise security
- Risk management
- Research and analysis
- Integration of computing, communications, and business disciplines

The CASP certified individual applies critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

It Pays to Get Certified

Certification is a great way to move ahead in your career and to gain more skills. Some ways that a certification can benefit you include:

In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

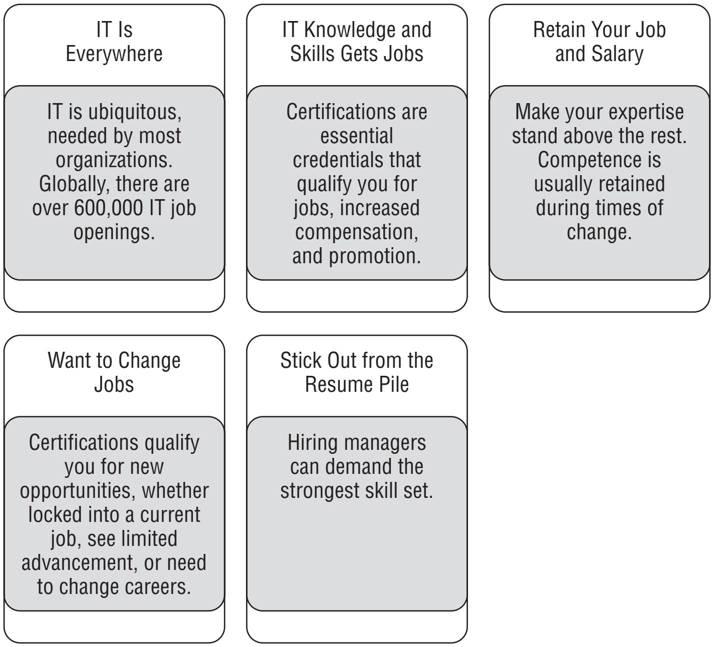
Security expertise is regularly required in organizations such as Hitachi Information Systems, Trend Micro, Lockheed Martin, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

Be the first. CASP is the first mastery level certification available from CompTIA. It expands on the widely recognized path of CompTIA Security+ with other 300,000 certified Security+ professionals.

The cloud is a new frontier. It requires astute security personnel who understand the security impact of the cloud on network design and risk.

Security is one of the job categories in highest demand. And this category is growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

How Certification Helps Your Career



IT Is Everywhere

IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.

IT Knowledge and Skills Gets Jobs

Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.

Retain Your Job and Salary

Make your expertise stand above the rest. Competence is usually retained during times of change.

Want to Change Jobs

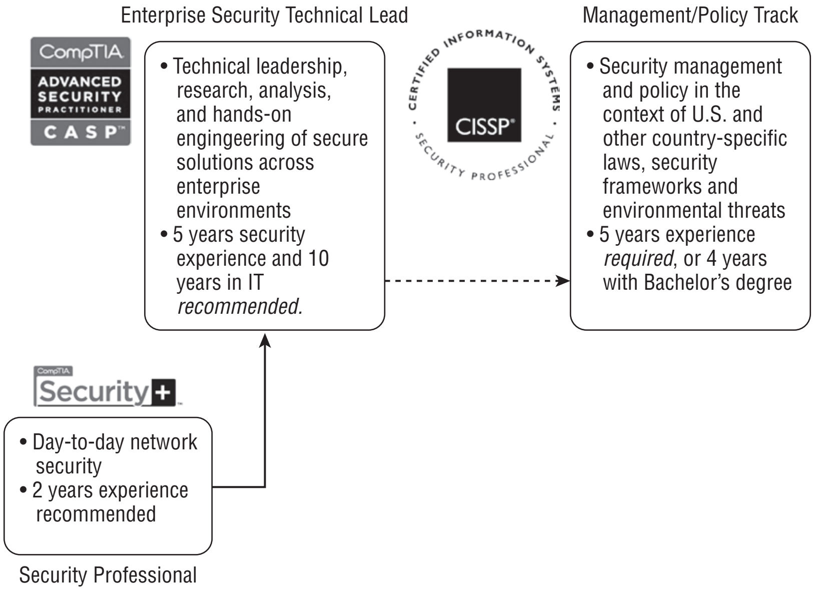
Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.

Stick Out from the Resume Pile

Hiring managers can demand the strongest skill set.

CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build on your skills and knowledge, supporting learning throughout your career.


Enterprise Security Technical Lead
CompTIA ADVANCED SECURITY PRACTITIONER CASP
• Technical leadership, research, analysis, and hands-on engingeering of secure solutions across enterprise environments
• 5 years security experience and 10 years in IT *recommended.*
Management/Policy Track
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP
• Security management and policy in the context of U.S. and other country-specific laws, security frameworks and environmental threats
• 5 years experience *required*, or 4 years with Bachelor's degree
CompTIA Security+
• Day-to-day network security
• 2 years experience recommended
Security Professional

Steps to Getting Certified

Review Exam Objectives Review the certification objectives to make sure you know what is covered in the exam. Visit `http://www.comptia.org/certifications/testprep/examobjectives.aspx`.

Practice for the Exam After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam. Visit `http://www.comptia.org/certifications/testprep/practicetests.aspx`.

Purchase an Exam Voucher Purchase your exam voucher on the CompTIA Marketplace, which is located at `www.comptiastore.com`.

Take the Test! Select a certification exam provider and schedule a time to take your exam. You can find exam providers here: `http://www.comptia.org/certifications/testprep/testingcenters.aspx`.

Stay Certified! Continuing Education The CASP certification is valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information, go to `http://certification.comptia.org/getCertified/certifications/casp.aspx`.

Join the IT Professional Community

The free IT Pro online community provides valuable content to students and professionals:

`http://itpro.comptia.org`

- Career IT job resources
  - Where to start in IT
  - Career assessments
  - Salary trends
  - US job search boards
- Forums on networking, security, computing, and cutting-edge technologies
- Access to blogs written by industry experts
- Current information on cutting-edge technologies
- Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This text bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100 percent of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives. Look for this seal on other materials you use to prepare for your certification exam.

Why CompTIA?

Global Recognition CompTIA is recognized globally as the leading IT nonprofit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.

Valued by Hiring Managers Hiring managers value CompTIA certification because it is a vendor- and technology-independent validation of your technical skills.

Recommended or Required by Government and Businesses Many government organizations and corporations either recommend or require technical staff to be CompTIA certified (e.g., Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more).

Three CompTIA Certifications Ranked in the Top 10 In a 2010 study by Dice.com of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to Obtain More Information

- Visit www.comptia.org to learn more about getting a CompTIA certification. And while you're at it, take a moment to learn a little more about CompTIA, the voice of the world's IT industry. Its membership includes companies on the cutting edge of innovation.
- To contact CompTIA with any questions or comments, please call 866-835-8020, ext. 5 or email questions@comptia.org.
- Social Media. Find CompTIA on:
  - Facebook
  - LinkedIn
  - Twitter
  - YouTube

Terry Erdle
Executive Vice President, Skills Certification,
CompTIA

Introduction

The CASP certification was developed by the Computer Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of security professionals who have ten years' experience in IT administration and at least five years' hands-on technical experience. The security professional's job is to protect the confidentiality, integrity, and availability of an organization's valuable information assets. As such, these individuals need to have the ability to apply critical thinking and judgment.

NOTE According to CompTIA, the CASP certification "is a vendor-neutral credential." The CASP validates "advanced-level security skills and knowledge" internationally. There is no prerequisite, but "CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, 'hands-on' focus at the enterprise level."

While many certification books present material for you to memorize before the exam, this book goes a step further in that it offers best practices, tips, and hands-on exercises that help those in the field of security better protect critical assets, build defense in depth, and accurately assess risk.

If you're preparing to take the CASP exam, it is a good idea to find as much information as possible about computer security practices and techniques. Because this test is designed for those with years of experience, you will be better prepared by having the most hands-on experience possible; this study guide was written with this in mind. We have included hands-on exercises, real-world scenarios, and review questions at the end of each chapter to give you some idea as to what the exam is like. You should be able to answer at least 90 percent of the test questions in this book correctly before attempting the exam; if you're unable to do so, reread the chapter and try the questions again. Your score should improve.

Before You Begin the CompTIA CASP Certification Exam

Before you begin studying for the exam, it's good for you to know that the CASP exam is offered by CompTIA (an industry association responsible for many certifications) and is granted to those who obtain a passing score on a single exam. Before you begin studying for the exam, learn all you can about the certification.

NOTE A detailed list of the CASP CAS-001 (2011 Edition) exam objectives is presented in this introduction; see the section "The CASP (2011 Edition) Exam Objectives."

Obtaining CASP certification demonstrates that you can help your organization design and maintain system and network security services designed to secure the organization's assets. By obtaining CASP certification, you show that you have the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments.

How to Become a CASP Certified Professional

As this book goes to press candidates can take the exam at any Pearson VUE testing center. The following table contains all the necessary contact information and exam-specific details for registering. Exam pricing might vary by country or by CompTIA membership.

Vendor	Website	Phone Number
Pearson VUE	`www.vue.com/comptia`	U.S. and Canada: 877-551-PLUS (7587)

Who Should Read This Book?

CompTIA Advanced Security Practitioner Study Guide is designed to give you insight into the working world of IT security and describes the types of tasks and activities that a security professional with five to ten years of experience carries out. Organized classes and study groups are the ideal structures for obtaining and practicing with the recommended equipment.

NOTE

College classes, training classes, and bootcamps offered by SANS and others are recommended ways to gain proficiency with the tools and techniques discussed in the book.