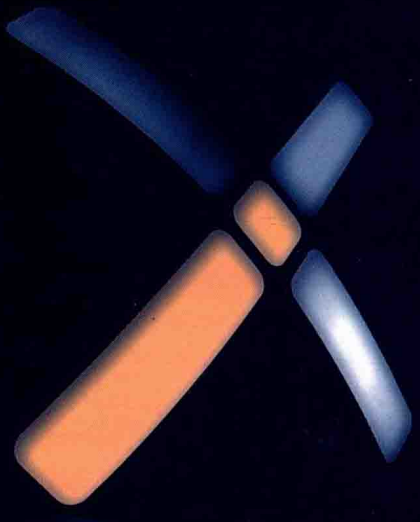
SYNGRESS

HCISPP Study Guide

Timothy Virtue
Justin Rainey



HCISPP Study Guide

Timothy Virtue
Justin Rainey

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress Publishers is an imprint of Elsevier

SYNGRESS

Acquiring Editor: Chris Katsaropoulos
Editorial Project Manager: Benjamin Rearick
Project Manager: Surya Narayanan Jayachandran
Designer: Maria Ines Cruz

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-802043-2

HCISPP Study Guide

Dedication

To my wife Jill – Your unconditional support and love make me the luckiest man alive. Thanks for sharing your life with me.

To my late grandpa Justin O'Connell whose 45 years of dedication teaching English at the University of Minnesota served as my inspiration to write this book.

Justin

To my late grandmothers Claire and Stella who showed me the importance of living life to the fullest, and that with passion and true grit, anything is possible.

Tim

Author Bio

Justin C. Rainey (CISSP, CIPP/US) is a global information security, privacy and technology risk management leader whose entire professional career has focused on the protection of nonpublic information. Justin began his career in 1998 providing security and technical support for an independent school district, and over the past 16 years, gained security and privacy experience in various areas including healthcare, research, education, telecommunications, retail, banking, insurance, and investment management. He currently serves as information security manager for a global investment management firm and is pursuing a bachelor of science degree in Political Science at the University of Houston. Justin resides in Houston, Texas with his wife Jill and their two dogs Austin and Mariette.

Tim Virtue (HCISPP, CISSP, CIPP/G, CISA, CCSK, CFE, CSM) is a global information security, privacy and risk management executive. Tim has extensive experience with publicly traded global corporations, privately held businesses, government agencies, and nonprofit organizations of all types and sizes. Tim holds an executive master of science in information systems technology degree from George Washington University and a bachelors of science in Criminal Justice degree with a concentration in security management from Northeastern University. He currently serves as the chief information security officer (CISO) for Texas.gov.

Technical Editor Bio

Jason Adamson (CEH, CISSP) is information security director for Voya Financial Services focusing on penetration testing, application code review, and other kinds of security testing. He has been working to protect PII and company sensitive data for 15 years and has worked for companies in financial, manufacturing, retail, and telecommunications sectors. Jason holds a degree in computer engineering technologies from Southern Polytechnic State University.

Preface

We are living in unprecedented times. This environment of constant change and transformation offers both opportunities and challenges. The opportunities and societal advances offered by healthcare technology are abundant. However, these advancements come with privacy and security concerns. We do not advocate fearing such change simply because of the privacy and security concerns. In fact, we look forward to all of the benefits and embrace the change, as long as society can find a way to balance the risks against the rewards. As we transition some of our most valued personal health information to various healthcare technology systems, there is and always will be a critical need for Information Security and Privacy professionals in the healthcare field.

There is a significant shortage of qualified professionals who truly understand all the aspects of Information Security and Privacy, including what it takes to develop, implement, and maintain an effective program while supporting the business needs of the organization and delivering leading-edge healthcare. We have seen a plethora of new threat actors enter the arena in an attempt to exploit vulnerable systems with various motives. These actors include foreign governments, "hacktivists," organized crime, cyber criminals, and even competitors in an attempt to gain a strategic advantage. The sophistication and scale of attacks surpass anything we've seen over the past decade and protecting healthcare organizations becomes more difficult as new technologies are adopted. This contributes to an insatiable demand for qualified Information Security and Privacy professionals.

Why focus on the Healthcare industry? Healthcare is growing at an unprecedented pace and is increasingly vulnerable as the industry shifts to electronic healthcare records.

The following is a list of key issues we believe will drive information security and privacy activities within the Healthcare industry and contribute to the demand for qualified professionals.

1. The Healthcare industry is extremely fragmented with minimal standards for interoperability and data sharing between hospitals, pharmacy benefit management companies, insurance companies, and

pharmacies. These issues are actively being addressed, but require a significant investment in technology. With increasing connectivity and access to systems and data, risks will also increase. Connectivity in the form of health information exchanges (HITS) and accountable care organizations also drives demand for qualified professionals.

2. There has been huge underinvestment in technology and especially for providers with most investments focused on providing or improving patient care. Old (legacy) systems remain a major security concern as many contain ePHI and need to be secured as they are updated or replaced.
3. There are enormous amounts of healthcare fraud and abuse within the industry, causing costs to spiral out of control. Technology in conjunction with security and privacy controls can provide solutions to increase business visibility and assist with managing these risks.
4. Demand for healthcare is exploding commensurate with the rapidly aging baby boomer population. This will require expansion of existing systems and implementation of new technologies to improve productivity and outcomes.
5. It is projected that the United States will experience a shortage of 160,000 doctors over the next 20 years and the industry will have to find new ways of improving doctor productivity. This will require implementation of new and innovative technologies that need to be secured.
6. Regulators have been aggressive in regulating the security and privacy of Healthcare IT systems and issuing fines for noncompliance.
7. Despite having vast amounts of sensitive data, healthcare Information Security programs are far behind that of Financial Services and other similarly situated industries. The FBI has also issued warnings to the Healthcare industry to urgently improve their programs and controls.
8. The Bureau of Labor Statistics (BLS) projects the job market for Information Security professionals to expand by 37% between 2012 and 2022. Information Security is one of the fastest-growing professions in the job market.

There are a vast number of opportunities for qualified healthcare Information Security and Privacy professionals. The HealthCare Certified Information Security and Privacy Practitioner (HCISPP) credential will certify your knowledge and stature as a qualified professional. There will be vast opportunities for those who prepare for the future, and this book is your first step toward a rewarding healthcare information security and privacy professional.

Acknowledgments

Justin would like to thank his wife, Jill, for her patience and support throughout the writing of this book. Thanks to co-author Tim Virtue and technical editor Jason Adamson for their contributions and collaboration on this work. And finally thanks to his family for their support: Kathleen Rainey, Edward Rainey, Scott Britain, and Dan and Allison Connally.

I would like to thank my family, friends, educators, and industry colleagues. Without your support, guidance, and mentorship over the years, I would not have the inspiration, expertise, or ability to write this book. I would also like to give a special thanks to co-author Justin Rainey, technical editor Jason Adamson, and the team at Elsevier. If not for their hard work, dedication, and support, we would not have had this book today.

Contents

CHAPTER 1

Introduction

THIS CHAPTER WILL HELP READERS UNDERSTAND

- Importance of information security and privacy
- Target audience
- HealthCare Information Security and Privacy Practitioner (HCISPP) certification requirements
- Learning objectives

BACKGROUND

The importance of security and privacy is rapidly increasing across all industries, especially given a recent acceleration in public data breach and record disclosures. As this book was composed the public has witnessed large breaches within the retail industry involving stolen credit card and personal information. At first glance one might discard this type of threat as not applicable to healthcare organizations given their core business involves the delivery of patient care. In many cases they might be wrong given patients regularly pay for healthcare services using a credit or debit card, the massive amount of personal health information (PHI) within the organization, a significant increase in the use of health information technology (which creates additional privacy and security risk), and PHI being shared outside organizational boundaries with third parties to support the delivery of healthcare services. Healthcare organizations will need qualified risk management professionals to assist with managing the broad array of risks faced within the industry. The HCISPP certification is for individuals who want to understand how to assess risk and implement and maintain security and privacy controls specific to the healthcare industry while being compliant with the many laws and regulations that govern the healthcare industry. Individuals with certifications such as the HCISPP are more likely to be selected for job interviews based on the immediate recognition of an industry certification and the qualifications it conveys. Since the

exam details are subject to change, per (ISC)², we encourage candidates to obtain the most current HCISPP Candidate Information Bulletin available from (ISC)2 prior to beginning their exam preparation. Candidates may require a deeper understanding of some concepts discussed throughout this book depending on the nature of their current or future roles, educational background, and work experience in each of the specific HCISPP exam domains. However, this book was written to provide a foundational level of knowledge and teach candidates only what is necessary to pass the HCISPP examination – nothing more, nothing less. Consider this the first step in a journey, as a security and privacy practitioner in the healthcare industry. Since the healthcare industry, the technology that supports it, and the laws and regulations that govern it continuously change we encourage HCISPP candidates and certificate holders to actively participate in the industry, stay abreast of changes, and commit to continuing education and gaining new experiences. The examination and this book focus on six key domains of knowledge:

- Healthcare industry
- Regulatory environment
- Privacy and security in healthcare
- Information governance and risk management
- Information risk assessment
- Third-party risk management

Individuals who may want to consider obtaining a HCISPP certification include, but are not limited to:

- Information security analysts
- Information security officers (CSO, CISO, ISO)
- Privacy officers (CPO)
- Compliance officers (CCO)
- Records management personnel
- Information technology managers
- Security and privacy consultants
- Risk management personnel
- Internal and external auditors
- Data protection officers
- Health information managers

HCISPP Certification Requirements

Prior to taking the HCISPP examination, candidates must meet the following requirements:

- Register for the exam and pay the examination fee. The most current fees are available at https://www.isc2.org/certification-register-now.aspx.

- Have a minimum of 2 years' security, privacy, and compliance experience in one of the six knowledge domains. At least 1 year of experience is required in one of the following three domains:
  - Healthcare industry
  - Regulatory environment in healthcare
  - Privacy and security in healthcare

The second year of experience can be in the domains mentioned earlier or in one of the following three domains:

- Information governance and risk management
- Information risk assessment
- Third-party risk management

Legal and information management experience may also be substituted for compliance and privacy experience, respectively.

- Provide a truthful attestation of professional experience and legally agree to abide by the Code of Ethics; and
- Provide yes or no responses to four questions pertaining to criminal history and background.

Exam Registration

The exam is computer-based (CBT) and proctored at an authorized location, while paper-based exams are available on a case-by-case basis. The exam will consist of 125 multiple choice questions with 4 potential choices and must be completed in 3 h. Candidates should ensure sufficient rest prior to the examination, and if traveling from outside the area, consider staying at a hotel close to the testing facility the night beforehand. Registration for the exam can be completed online through the (ISC)2 website or over the phone and requires payment of the exam fee, agreement to the Code of Ethics, and responses to criminal history and background questions.

Code of Ethics

The Code of Ethics includes a preamble and four cannons focused on ethics. All professionals who receive an HCISPP certification must abide by the Code, recognize their certification is a privilege (not a right), and understand the certification is subject to revocation for members who intentionally or knowingly violate the Code.

Preamble

The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the