

5th Edition



Systems Security Certified Practitioner

An (ISC)² Certification

The Official (ISC)²
SSCP CBK[®] Reference

Mike Wills

 **SYBEX[®]**
A Wiley Brand

The Official (ISC)²[®] SSCP[®] CBK[®] Reference

Fifth Edition

The Official (ISC)²[®] SSCP[®] CBK[®] Reference

Fifth Edition

MIKE WILLS



Copyright © 2020 by (ISC)²

Portions of this Work are reused from (ISC)² SSCP Systems Security Certified Practitioner Official Study Guide, 2nd Edition by Mike Wills copyright 2019 John Wiley & Sons, Inc.

Portions of this Work are reused from The Official (ISC)² Guide to the CISSP CBK Reference, 5th Edition by John Warsinske with Mark Graff, Kevin Henry, Christopher Hoover, Ben Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl, Mike Vasquez copyright 2019 (ISC)²

Published by John Wiley & Sons, Inc. Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-60194-4

ISBN: 978-1-119-60196-8 (ebk.)

ISBN: 978-1-119-60200-2 (ebk.)

Manufactured in the United States of America

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

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 publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019952065

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. (ISC)², SSCP, and CBK are registered trademarks or certification marks of International Information Systems Certification Consortium, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Acknowledgments

“It’s like writing two books at once, only harder,” Jim said to me when he asked me to take on writing this Common Book of Knowledge book while I was still writing the SSCP Study Guide. More like taking one subject, turning it sideways, and shaking hard, perhaps! Unlike the Study Guide, writing this book felt more like writing several hundred short white papers on closely related subjects.

Since this book needed to speak to troubleshooters, I drew on decades of teaching I’d received from many professionals in the military, in government, and in the private sector about the fine art and brute-force cybernetics of debugging networks, systems, highly secure communications systems, and all of the arcana of controlling space-based systems working many different missions. I’ve also drawn on years of working with small and medium but otherwise rather down-to-earth business IT systems and what it took to get them back into operations. Where that problem-solving focus comes through clearly and helps you shoot the troubles you have to deal with, I owe a great debt of thanks to those who let me learn how in real time.

Without the tireless support of the editorial team at Wiley/Sybex—Jim Minatel and Kelly Talbot—I think I’d *still* be struggling with unflowing the lessons and reflowing them into reference and troubleshooting memory-joggers. And as with producing the Study Guide, the technical review by Jacob Penovich, as well as by Tara Zeiler and Charles Gaughf at (ISC)², have all helped make what you have in your hands right now deliver the right content in the best way possible. Christine O’Connor, Kim Wimpsett and the rest of her team of proofreaders and copyeditors made it all look great too! Any remaining mistakes, omissions, or confusing passages that remain are mine, not theirs; let me know please when you find one!

Finally, I wish to thank my wife Nancy. She saved my life and brought me peace. Her strength inspired me to say “yes” one more time when Jim called me, again, about doing this book, and she has kept both of us healthy and happy throughout. We go together, on adventures like writing, and on ones for which we do need to pack a pocket handkerchief.

About the Author



Mike Wills, SSCP, CISSP, CAMS, has spent more than 40 years as a computer systems architect, programmer, security specialist, database designer, consultant, and teacher (among other duties). Starting out as a bit of a phone phreak in his college days, he sharpened his skills on the 1960s generation of mainframes and minicomputers, just in time for the first 8080 and Z80 microprocessors to fuel the home computer revolution. Learning about the ARPANET just added spice to that mix. Since then, he's had ones, zeros, and now qubits under his fingernails too many times to count, whether as part of his jobs, his teaching, or his hobbies.

Mike earned his BS and MS degrees in computer science, both with minors in electrical engineering, from the Illinois Institute of Technology; and his MA in defence studies from King's College, London. He is a graduate of the Federal Chief Information Officer program at National Defense University and the Program Manager's Course at Defense Systems Management College.

As an Air Force officer, Mike served in the National Reconnaissance Office, building and flying some of the most complex, cutting-edge space-based missions large and small. As a “ground control” guy, he specialized in the design, operation, and support of highly secure, globe-spanning command, control, communications and intelligence systems that support U.S. and Coalition missions around the world. These duties often required Mike to “optimize” his way around the official configuration management and security safeguards—all on official business, of course.

Because no good deed goes unpunished, he then spent two years on the Joint Staff as a policy and budget broker for all command, control, and communications systems, and then taught in the School of Information Warfare and Strategy at National Defense University. He's taught at senior leader colleges in both the United States and United Kingdom and has been a continuing guest lecturer at the UK's Defence Academy. He served as advisor to the United Kingdom's Joint Intelligence Committee, Ministry of Justice, and Defence Science and Technology Laboratories on the national and personal security implications of science and technology policy; this led to him sometimes being known as the United Kingdom's nonresident expert on outer space law.

Mike is the author of the *SSCP Official Study Guide 2nd Edition*. Along with his SSCP and CISSP, Mike is also a Certified Anti-Money Laundering Specialist.

Currently he is an assistant professor of applied information technologies in the College of Business at Embry-Riddle Aeronautical University, Worldwide Campus, where he is the change

leader and academic visionary behind bringing the Microsoft Software and Systems Academy program into ERAU's classrooms at 13 locations around the United States. Prior to this, Mike helped create two new master of science degrees—information security and assurance, and management of information systems—and was program chair of both during their launch and first year of teaching. He also taught in Worldwide's Security and Intelligence Studies program during its 2005 launch in ERAU's European Division.

Mike and his wife Nancy currently call Montevideo, Uruguay, their home. Living abroad since the end of the last century, they find new perspectives, shared values, and wonderful people wherever they go. As true digital nomads, it's getting time to move again. Where to? They'll find out when they get there.

About the Technical Editor

Jacob Penovich is an experienced information security practitioner who has worked in a variety of roles from systems administration to ethical hacking and penetration testing. Jacob is driven by a strong belief in the practice of empowering team members, colleagues, and the local InfoSec community while striving to help cultivate an environment of knowledge exchange and growth.

Holder of numerous industry certifications including the CISSP, GPEN, GWAPT, and more, he considers himself a lifelong learner who is always on the lookout for unique challenges, upcoming threats, and new ways to approach InfoSec issues. He loves to volunteer and give back whenever possible and enjoys working with local high schools and colleges to help inspire the next generation of InfoSec pros. When not absorbed in a computer screen, he can be found in the company of his amazing wife Jessica and their grumble of pugs.

Contents at a Glance

Foreword	xxi
Introduction	xxiii
CHAPTER 1: ACCESS CONTROLS	1
CHAPTER 2: SECURITY OPERATIONS AND ADMINISTRATION	65
CHAPTER 3: RISK IDENTIFICATION, MONITORING, AND ANALYSIS	147
CHAPTER 4: INCIDENT RESPONSE AND RECOVERY	247
CHAPTER 5: CRYPTOGRAPHY	335
CHAPTER 6: NETWORK AND COMMUNICATIONS SECURITY	467
CHAPTER 7: SYSTEMS AND APPLICATION SECURITY	649
Index	731

Contents

Foreword	xxi
Introduction	xxiii
CHAPTER 1: ACCESS CONTROLS	1
Access Control Concepts	3
Subjects and Objects	4
Privileges: What Subjects Can Do with Objects	6
Data Classification and Access Control	7
Access Control via Formal Security Models	9
Implement and Maintain Authentication Methods	12
Single-Factor/Multifactor Authentication	13
Accountability	32
Single Sign-On	34
Device Authentication	35
Federated Access	36
Support Internetwork Trust Architectures	38
Trust Relationships (One-Way, Two-Way, Transitive)	39
Extranet	40
Third-Party Connections	41
Zero Trust Architectures	42
Participate in the Identity Management Lifecycle	43
Authorization	44
Proofing	45
Provisioning/Deprovisioning	46
Identity and Access Maintenance	48
Entitlement	52
Identity and Access Management Systems	55
Implement Access Controls	58
Mandatory, Discretionary, and Nondiscretionary	59
Role-Based	61
Attribute-Based	62

Subject-Based	62
Object-Based	62
Summary	63
CHAPTER 2: SECURITY OPERATIONS AND ADMINISTRATION	65
Comply with Codes of Ethics	66
Understand, Adhere to, and Promote Professional Ethics	67
(ISC) ² Code of Ethics	68
Organizational Code of Ethics	69
Understand Security Concepts	70
Conceptual Models for Information Security	71
Confidentiality	72
Integrity	79
Availability	81
Accountability	82
Privacy	82
Nonrepudiation	90
Authentication	91
Safety	92
Key Control Principles	93
Access Control and Need-to-Know	98
Job Rotation and Privilege Creep	99
Document, Implement, and Maintain Functional Security Controls	101
Deterrent Controls	101
Preventative Controls	103
Detective Controls	103
Corrective Controls	104
Compensating Controls	105
The Lifecycle of a Control	106
Participate in Asset Management	107
Asset Inventory	108
Lifecycle (Hardware, Software, and Data)	111
Hardware Inventory	112
Software Inventory and Licensing	113
Data Storage	114
Implement Security Controls and Assess Compliance	120
Technical Controls	121
Physical Controls	122

Administrative Controls	125
Periodic Audit and Review	128
Participate in Change Management	130
Execute Change Management Process	132
Identify Security Impact	134
Testing/Implementing Patches, Fixes, and Updates	134
Participate in Security Awareness and Training	135
Security Awareness Overview	136
Competency as the Criterion	137
Build a Security Culture, One Awareness Step at a Time	137
Participate in Physical Security Operations	138
Physical Access Control	138
The Data Center	142
Service Level Agreements	143
Summary	146
 CHAPTER 3: RISK IDENTIFICATION, MONITORING, AND ANALYSIS	 147
Defeating the Kill Chain One Skirmish at a Time	148
Kill Chains: Reviewing the Basics	151
Events vs. Incidents	155
Understand the Risk Management Process	156
Risk Visibility and Reporting	159
Risk Management Concepts	165
Risk Management Frameworks	185
Risk Treatment	195
Perform Security Assessment Activities	203
Security Assessment Workflow Management	204
Participate in Security Testing	206
Interpretation and Reporting of Scanning and Testing Results	215
Remediation Validation	216
Audit Finding Remediation	217
Manage the Architectures: Asset Management and Configuration Control	218
Operate and Maintain Monitoring Systems	220
Events of Interest	222
Logging	229
Source Systems	230
Legal and Regulatory Concerns	236
Analyze Monitoring Results	238
Security Baselines and Anomalies	240

Visualizations, Metrics, and Trends	243
Event Data Analysis	244
Document and Communicate Findings	245
Summary	246
CHAPTER 4: INCIDENT RESPONSE AND RECOVERY	247
Support the Incident Lifecycle	249
Think like a Responder	253
Physical, Logical, and Administrative Surfaces	254
Incident Response: Measures of Merit	254
The Lifecycle of a Security Incident	255
Preparation	257
Detection, Analysis, and Escalation	264
Containment	275
Eradication	277
Recovery	279
Lessons Learned; Implementation of New Countermeasures	283
Third-Party Considerations	284
Understand and Support Forensic Investigations	287
Legal and Ethical Principles	289
Logistics Support to Investigations	291
Evidence Handling	292
Evidence Collection	297
Understand and Support Business Continuity Plan and Disaster Recovery Plan Activities	306
Emergency Response Plans and Procedures	307
Interim or Alternate Processing Strategies	310
Restoration Planning	313
Backup and Redundancy Implementation	315
Data Recovery and Restoration	319
Training and Awareness	321
Testing and Drills	322
CIANA at Layer 8 and Above	328
It Is a Dangerous World Out There	329
People Power and Business Continuity	332
Summary	333
CHAPTER 5: CRYPTOGRAPHY	335
Understand Fundamental Concepts of Cryptography	336
Building Blocks of Digital Cryptographic Systems	339
Hashing	347

Salting	351
Symmetric Block and Stream Ciphers	353
Stream Ciphers	365
EU ECRYPT	371
Asymmetric Encryption	371
Elliptical Curve Cryptography	380
Nonrepudiation	383
Digital Certificates	388
Encryption Algorithms	392
Key Strength	393
Cryptographic Attacks, Cryptanalysis, and Countermeasures	395
Cryptologic Hygiene as Countermeasures	396
Common Attack Patterns and Methods	401
Secure Cryptoprocessors, Hardware Security Modules, and Trusted Platform Modules	409
Understand the Reasons and Requirements for Cryptography	414
Confidentiality	414
Integrity and Authenticity	415
Data Sensitivity	417
Availability	418
Nonrepudiation	418
Authentication	420
Privacy	421
Safety	422
Regulatory	423
Transparency and Auditability	423
Competitive Edge	424
Understand and Support Secure Protocols	424
Services and Protocols	425
Common Use Cases	437
Deploying Cryptography: Some Challenging Scenarios	442
Limitations and Vulnerabilities	444
Understand Public Key Infrastructure Systems	446
Fundamental Key Management Concepts	447
Hierarchies of Trust	459
Web of Trust	462
Summary	464

CHAPTER 6: NETWORK AND COMMUNICATIONS SECURITY	467
Understand and Apply Fundamental Concepts of Networking	468
Complementary, Not Competing, Frameworks	470
OSI and TCP/IP Models	471
OSI Reference Model	486
TCP/IP Reference Model	501
Converged Protocols	508
Software-Defined Networks	509
IPv4 Addresses, DHCP, and Subnets	510
IPv4 Address Classes	510
Subnetting in IPv4	512
Running Out of Addresses?	513
IPv4 vs. IPv6: Key Differences and Options	514
Network Topographies	516
Network Relationships	521
Transmission Media Types	525
Commonly Used Ports and Protocols	530
Understand Network Attacks and Countermeasures	536
CIANA+PS Layer by Layer	538
Common Network Attack Types	553
SCADA, IoT, and the Implications of Multilayer Protocols	562
Manage Network Access Controls	565
Network Access Control and Monitoring	568
Network Access Control Standards and Protocols	573
Remote Access Operation and Configuration	575
Manage Network Security	583
Logical and Physical Placement of Network Devices	586
Segmentation	587
Secure Device Management	591
Operate and Configure Network-Based Security Devices	593
Network Address Translation	594
Additional Security Device Considerations	596
Firewalls and Proxies	598
Network Intrusion Detection/Prevention Systems	605
Security Information and Event Management Systems	607
Routers and Switches	609
Network Security from Other Hardware Devices	610
Traffic-Shaping Devices	613

Operate and Configure Wireless Technologies	615
Wireless: Common Characteristics	616
Wi-Fi	624
Bluetooth	637
Near-Field Communications	638
Cellular/Mobile Phone Networks	639
Ad Hoc Wireless Networks	640
Transmission Security	642
Wireless Security Devices	645
Summary	646
CHAPTER 7: SYSTEMS AND APPLICATION SECURITY	649
Systems and Software Insecurity	650
Software Vulnerabilities Across the Lifecycle	654
Risks of Poorly Merged Systems	663
Hard to Design It Right, Easy to Fix It?	664
Hardware and Software Supply Chain Security	667
Positive and Negative Models for Software Security	668
Is Blacklisting Dead? Or Dying?	669
Information Security = Information Quality + Information Integrity	670
Data Modeling	671
Preserving Data Across the Lifecycle	674
Identify and Analyze Malicious Code and Activity	678
Malware	679
Malicious Code Countermeasures	682
Malicious Activity	684
Malicious Activity Countermeasures	688
Implement and Operate Endpoint Device Security	689
HIDS	691
Host-Based Firewalls	692
Application White Listing	693
Endpoint Encryption	694
Trusted Platform Module	695
Mobile Device Management	696
Secure Browsing	697
IoT Endpoint Security	700
Operate and Configure Cloud Security	701
Deployment Models	702
Service Models	703

Virtualization	706
Legal and Regulatory Concerns	709
Data Storage and Transmission	716
Third-Party/Outsourcing Requirements	716
Lifecycles in the Cloud	717
Shared Responsibility Model	718
Layered Redundancy as a Survival Strategy	719
Operate and Secure Virtual Environments	720
Software-Defined Networking	723
Hypervisor	725
Virtual Appliances	726
Continuity and Resilience	727
Attacks and Countermeasures	727
Shared Storage	729
Summary	730
Index	731

Foreword



WELCOME TO THE OFFICIAL (ISC)² *Guide to the SSCP CBK*! By picking up this book, you've made the decision to take the next step in your career and have demonstrated your commitment to continuing your professional education.

The recognition that comes with an (ISC)² Systems Security Certified Practitioner (SSCP) credential next to your name shows your understanding of and proficiency with the hands-on technical work that is needed in the information security field. It demonstrates that you closely follow best practices, policies and procedures in accordance with the *SSCP Common Body of Knowledge*. Whether you are using this guide to supplement your preparation to sit for the exam or you are an existing SSCP using this as a reference, this book helps to facilitate the practical knowledge you need to assure strong information security for your organization's daily operations.

The recognized leader in the field of information security education and certification, (ISC)² promotes the development of information security professionals throughout the world. As a SSCP with all the benefits of (ISC)² membership, you will become part of a global network of more than 140,000 certified professionals who are working to inspire a safe and secure cyber world. By becoming a member of (ISC)² you will have also officially committed to ethical conduct commensurate to your position of trust as a cybersecurity professional.

Reflecting the most pertinent issues that security practitioners currently face, along with the best practices for mitigating those issues, *The Official (ISC)² Guide to the SSCP CBK* offers step-by-step guidance through the seven different domains included in the exam, which are:

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring and Analysis
- Incident Response and Recovery
- Cryptography
- Networks and Communications Security
- Systems and Application Security

Drawing from a comprehensive, up-to-date global body of knowledge, this book prepares you to join thousands of practitioners worldwide who have obtained the SSCP. For those with proven technical skills and practical security knowledge, the SSCP certification is the ideal credential. The SSCP confirms the breadth and depth of practical security knowledge expected of those in hands-on operational IT roles. The certification provides industry-leading confirmation of a practitioner's ability to implement, monitor and administer information security policies and procedures that ensure data confidentiality, integrity and availability (CIA).

The goal for SSCP credential holders is to achieve the highest standard for cybersecurity expertise – managing multi-platform IT systems while keeping sensitive data secure. This becomes especially crucial in the era of digital transformation, where cybersecurity permeates virtually every value stream imaginable. Organizations that can demonstrate world-class cybersecurity capabilities and trusted transaction methods enable customer loyalty and fuel success.

The opportunity has never been greater for dedicated men and women to carve out a meaningful career and make a difference in their organizations. *The Official (ISC)² Guide to the SSCP CBK* will be your constant companion in protecting and securing the critical data assets of your organization that will serve you for years to come.

Thank you for reading and good luck in this next step along your career path.

Regards,

A handwritten signature in black ink, reading "David P. Shearer". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

David P. Shearer, CISSP
CEO, (ISC)²

Introduction

CONGRATULATIONS ON CHOOSING TO become a Systems Security Certified Practitioner (SSCP)! In making this choice, you’re signing up to join the “white hats,” the professionals who strive to keep our information-based modern world safe, secure, and reliable. SSCPs and other information security professionals help businesses and organizations keep private data *private* and help to ensure that published and public-facing information stays unchanged and unhacked.

Whether you are new to the fields of information security, information assurance, or cybersecurity, or you’ve been working with these concepts, tools, and ideas for some time now, this book is here to help you grow your knowledge, skills, and abilities as a systems security professional.

Let’s see how!

ABOUT THIS BOOK

You’re here because you need a ready reference source of ideas, information, knowledge, and experience about information systems security. Users of earlier editions of the CBK describe it as the place to go when you need to look up something about bringing your systems or networks back up and online—when you can’t exactly Google or Bing it. As a first responder in an information security incident, you may need to rely on what you know and what you’ve got at hand as you characterize, isolate, and contain an intruder and their malware or other causal agents. This book cannot answer all of the questions you’ll have in real time, but it may just remind you of important concepts as well as critical details when you need them. As with any reference work, it can help you think your way through to a solution. By taking key definitions and concepts and *operationalizing* them, showing how they work in practice, this book can enrich the checklists, troubleshooting guides, and task-focused procedures that you may already be using in your work.

✓ Why This CBK as Well as a Study Guide?

Good question! This Common Book of Knowledge (CBK) provides you the data, information, knowledge—and in some cases, some bits of wisdom—that have been hard-won by the experience of many SSCPs and other information security professionals. This CBK is structured around the SSCP domains of knowledge; as such, it's not a cover-to-cover learning journey but more of an atlas for such a journey.

The SSCP Official Study Guide exists because (ISC)² wanted a book that would teach as well as guide, explain as well as capture the common knowledge about keeping information systems secure, protecting information assets, and information assurance that all SSCPs should have at their mental fingertips. As creators of the SSCP program, (ISC)² defines that common body of knowledge, in continuous consultation with system security experts and practitioners from business, industry, government, and academia from around the world. This book is its natural companion.

The SSCP Seven Domains

This book directly reflects the SSCP Common Body of Knowledge, which is the comprehensive framework that (ISC)² has developed to express what security professionals should have working knowledge of. These domains include theoretical knowledge, industry best practices, and applied skills and techniques. Chapter by chapter, this book takes you through these domains, with major headings within each chapter being your key to finding what you need when you need it. Topics that are covered in more than one domain will be found within sections or subsections in each chapter as appropriate.

(ISC)² is committed to helping members learn, grow, and thrive. The Common Body of Knowledge (CBK) is the comprehensive framework that helps (ISC)² fulfill this commitment. The CBK includes all the relevant subjects a security professional should be familiar with, including skills, techniques, and best practices. (ISC)² uses the various domains of the CBK to test a certificate candidate's levels of expertise in the most critical aspects of information security. You can see this framework in the SSCP Exam Outline at www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/SSCP-Exam-Outline-Nov-1-2018.ashx.

Chapter by chapter, domain by domain, these domains are as follows:

Chapter 1: Access Controls Policies, standards, and procedures that define who users are, what they can do, which resources and information they can access, and what operations they can perform on a system, such as:

- 1.1 Implement and maintain authentication methods
- 1.2 Support internetwork trust architectures

1.3 Participate in the identity management life cycle

1.4 Implement access controls

Chapter 2: Security Operations and Administration Identification of information assets and documentation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability, such as:

2.1 Comply with codes of ethics

2.2 Understand security concepts

2.3 Document, implement, and maintain functional security controls

2.4 Participate in asset management

2.5 Implement security controls and assess compliance

2.6 Participate in change management

2.7 Participate in security awareness and training

2.8 Participate in physical security operations

Chapter 3: Risk Identification, Monitoring, and Analysis Risk identification is the review, analysis, and implementation of processes essential to the identification, measurement, and control of loss associated with unplanned adverse events. Monitoring and analysis consists of determining system implementation and access in accordance with defined IT criteria. Collecting information for identification of, and response to, security breaches or events, such as the following:

3.1 Understand the risk management process

3.2 Perform security assessment activities

3.3 Operate and maintain monitoring systems

3.4 Analyze monitoring results

Chapter 4: Incident Response and Recovery The show must go on is a well-known saying that means, even if there are problems or difficulties, an event or activity must continue. Incident response and recovery ensures the work of the organization will continue. In this domain the SSCP gains an understanding of how to handle incidents using consistent, applied approaches like business continuity planning (BCP) and disaster recovery planning (DRP). These approaches are utilized to mitigate damages, recover business operations, and avoid critical business interruption.

4.1 Support incident life cycle

4.2 Understand and support forensic investigations

4.3 Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) activities

Chapter 5: Cryptography The protection of information using techniques that ensure its integrity, confidentiality, authenticity, and nonrepudiation, and the recovery of encrypted information in its original form.

5.1 Understand fundamental concepts of cryptography

5.2 Understand reasons and requirements for cryptography

5.3 Understand and support secure protocols

5.4 Understand Public Key Infrastructure (PKI) systems

Chapter 6: Network and Communications Security The network structure, transmission methods and techniques, transport formats, and security measures used to operate both private and public communication networks.

6.1 Understand and apply fundamental concepts of networking

6.2 Understand network attacks and countermeasures

6.3 Manage network access controls

6.4 Manage network security

6.5 Operate and configure network-based security devices

6.6 Operate and configure wireless technologies

Chapter 7: Systems and Application Security Countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses, and other related forms of intentionally created damaging code.

7.1 Identify and analyze malicious code and activity

7.2 Implement and operate endpoint device security

7.3 Operate and configure cloud security

7.4 Operate and secure virtual environments

Using This Book to Defeat the Cybersecurity Kill Chain

Your employers or clients have entrusted the safety and security of their information systems to you, as one of their on-site information security professionals. Those systems are under constant attack—not just the threat of attack. Each day, the odds are great that somebody is knocking at your electronic front doors, trying the e-window latches on your organization’s web pages, and learning about your information systems and how you use them. That’s reconnaissance in action, the first step in the cybersecurity kill chain.

As an SSCP you’re no doubt aware of the cybersecurity kill chain, as a summary of how advanced persistent threat (APT) actors plan and conduct their attacks against many private and public organizations, their IT infrastructures, and their information assets and systems. Originally developed during the 1990s by applying military planning doctrines

of effects-based targeting, this kill chain is similar to the value chain concept used by businesses and public-sector organizations around the world. Both value chains and kill chains start with the objective—the desired end state or result—and work backward, all the way back to choosing the right targets to attack in the first place.¹ Lockheed-Martin first published its cybersecurity kill chain in 2011; the MITRE Corporation, a federally funded research and development corporation (FFRDC), expanded on this in 2018 with its threat-based Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. ATT&CK takes the kill chain concept down into the tactics, techniques, and procedures used by squad-level and individual soldiers in the field. (Note that in military parlance, planning flows from strategic, through operational, to tactical; but common business-speak usage flips the names of the last two steps, looking at business operations as being the point-of-contact steps with customers, and the tactical layer of planning translating strategic objectives into manageable, measurable, value-producing packages of work.) ATT&CK as a framework is shown in Figure 1, highlighting the two major phases that defenders need to be aware of and engaged with: prestrike planning and the enterprise-level targeted strikes at your systems, your data, and your mission.

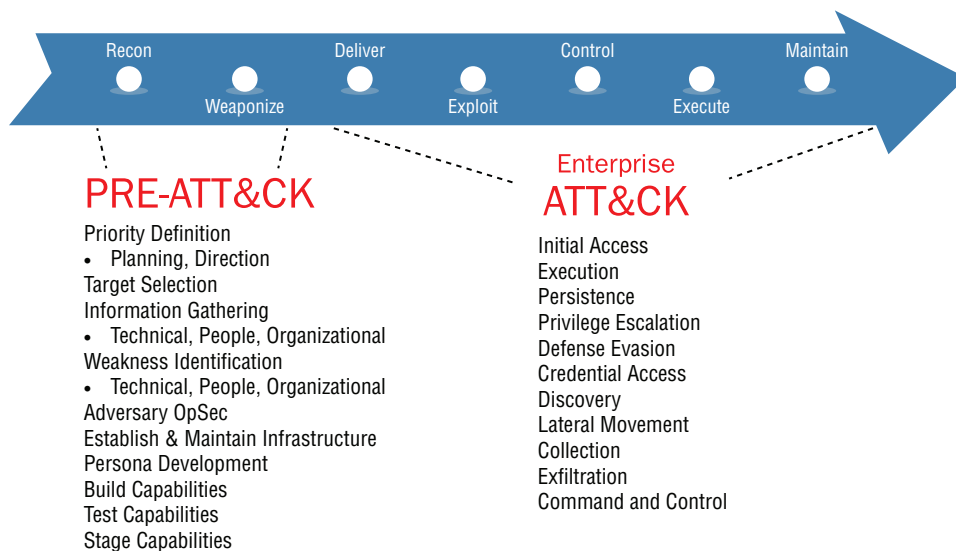


FIGURE 1 MITRE's ATT&CK cybersecurity kill chain model © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

¹I had the privilege of developing and teaching some of these evolving concepts at the U.S. National Defense University's School of Information Warfare and Strategy, 1998-2000. At the School, we made extensive use of the "Strategic Information Warfare" series of publications by Roger C. Molander and others at the RAND Corporation, which were exploring this backward chain from desired strategic effect to the "kill effect" required of attacks on information and information systems.

MITRE, Lockheed Martin, and others may give slightly different names to the different phases of their kill chain models. For example, MITRE’s combines exploitation with installation, while emphasizing the persistent presence of the adversary inside your systems as they maintain their capabilities to quietly wreak havoc and achieve their objectives. The names of the phases aren’t important; their underlying flow of ideas is what matters. To date, there does not seem to be any evidence that any given attacker has used exactly one planning model or another. There is abundant evidence, however, that defenders who do not understand these models pay for their ignorance—or, more precisely, their employers and clients do.

Combining these two models gives us eight phases of the life of an APT’s kill chain and suggests which domains of knowledge (and therefore which chapters) may be your first ports of call as you plan to detect, prevent, degrade, or defeat the individual tasks that might make up each step in such a kill chain’s operation. These are shown in Table 1.

TABLE 1 Kill Chain Phases Mapped to Chapters

KILL CHAIN PHASE	ATTACK OPERATIONS	DEFENSIVE OPTIONS
Reconnaissance	All-source intelligence gathering to inform the attack: OSINT, scanning, early intrusion, social engineering	All chapters: enhance overall risk/security posture, awareness, vigilance
Weaponization	Select and prepare access techniques and pathways	Chapters 1, 7
Delivery	Email, USBs, URLs, access control gaps, etc.	Chapters 1, 2, 5, 6, 7
Exploitation	Malware, rootkit exploits, live off the land	Chapters 1, 4, 6, 7
Installation	Backdoors, false or subverted user IDs	Chapters 1, 7
Command & Control	Privilege escalation, credential access; lateral movement; find, fix, select in-system targets	Chapters 1, 2, 4, 6
Execute the Attack	Exfiltrate; corrupt; encrypt for ransom; springboard to other targets	Chapters 4, 5
Maintain Hostile Presence	Continue to exploit target’s systems and data; continue hiding one’s tracks	Chapters 1, 4, 6, 7

You might be wondering why all chapters seem to apply to the Reconnaissance phase. The key to this is to recognize that the attacker will seek to find all possible sources of information about your organization, its business associates and relationships, its communications patterns, and its IT systems. APTs seek understanding of their targets’ business and social networks, the “watering holes” where their people gather to collaborate with