

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
<https://doi.org/10.1007/978-1-4842-3258-3>

ISBN-13 (electronic): 978-1-4842-3258-3

Library of Congress Control Number: 2018935923

Copyright © 2018 by Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

About the Authors.....	xxiii
About this Study Guide	xxv
Introduction	xxxiii
Part I: The Cybersecurity Challenge	1
Chapter 1: Defining the Cybersecurity Challenge	3
Chapter 2: Meeting the Cybersecurity Challenge	53
Part II: A New Enterprise Cybersecurity Architecture	93
Chapter 3: Enterprise Cybersecurity Architecture.....	95
Chapter 4: Implementing Enterprise Cybersecurity	135
Chapter 5: Operating Enterprise Cybersecurity	173
Chapter 6: Enterprise Cybersecurity and the Cloud.....	219
Chapter 7: Enterprise Cybersecurity for Mobile and BYOD.....	249
Part III: The Art of Cyberdefense.....	275
Chapter 8: Building an Effective Defense	277
Chapter 9: Responding to Incidents	313
Chapter 10: Managing a Cybersecurity Crisis	333
Part IV: Enterprise Cyberdefense Assessment.....	377
Chapter 11: Assessing Enterprise Cybersecurity	379
Chapter 12: Measuring a Cybersecurity Program	407
Chapter 13: Mapping Against Cybersecurity Frameworks	429
Part V: Enterprise Cybersecurity Program.....	449
Chapter 14: Managing an Enterprise Cybersecurity Program	451
Chapter 15: Looking to the Future	487

CONTENTS AT A GLANCE

Part VI: Appendices	513
Appendix A: Sample Cybersecurity Policy	515
Appendix B: Cybersecurity Operational Processes.....	545
Appendix C: Object Measurement.....	565
Appendix D: Cybersecurity Sample Assessment	603
Appendix E: Cybersecurity Capability Value Scales	663
Index.....	701

Contents

About the Authors.....	xxiii
About this Study Guide	xxv
Introduction	xxxiii
Part I: The Cybersecurity Challenge	1
Chapter 1: Defining the Cybersecurity Challenge	3
Overview	4
Topics.....	6
The Cyberattacks of Today	7
Context	7
The Sony Pictures Entertainment Breach of 2014.....	8
Advanced Persistent Threats	9
Waves of Malware	10
Types of Cyberattackers.....	12
Context	12
Commodity Threats.....	13
Hacktivists	14
Organized Crime	15
Espionage	17
Cyberwar	18
Types of Cyberattacks	19
Context	19
Confidentiality—Steal Data	21
Integrity—Modify Data	22
Availability—Deny Access to Data, Services, or Systems	23
The Steps of a Cyberintrusion.....	24
Attack Trees and Attack Graphs.....	24
Lockheed Martin Kill Chain.....	26

CONTENTS

Mandiant Attack Life Cycle	29
Enterprise Cybersecurity Attack Sequence	32
Why Cyberintrusions Succeed	35
Context	35
The Explosion in Connectivity	36
Consolidation of Enterprise IT	37
Defeat of Protective Controls/Failure of Detective Controls	38
Defeat of Preventive Controls	39
Failure of Detective Controls	40
Compliance over Capability	41
The Gap in Cybersecurity Effectiveness	42
A New Cybersecurity Mindset	43
An Effective Enterprise Cybersecurity Program	46
Rest of Study Guide	51
Chapter 2: Meeting the Cybersecurity Challenge	53
Overview	54
Topics	56
Cybersecurity Frameworks	57
Representative Frameworks	57
Commonalities of Cybersecurity Frameworks	58
The Cybersecurity Process	59
Cybersecurity Challenges	62
NIST Special Publication 800-53 Revision 4	62
The Risk Management Process	65
Vulnerabilities, Threats, and Risks	69
Risk Analysis and Mitigation	71
Reducing the Probability of an Incident and/or the Impact of an Incident	71
Cybersecurity Controls	73
Context	73
Cybersecurity Capabilities	78
Cybersecurity and Enterprise IT	80
Context	80
Endpoints	81
IT Infrastructure	83

Emplacing Cyberdefenses.....	84
How Cyberdefenses Interconnect	86
An Enterprise Cybersecurity Architecture	89
Context	89
Part II: A New Enterprise Cybersecurity Architecture	93
Chapter 3: Enterprise Cybersecurity Architecture.....	95
Overview	96
Topics.....	98
Systems Administration	99
Network Security	102
Application Security	105
Endpoint, Server, and Device Security	108
Identity, Authentication, and Access Management.....	111
Data Protection and Cryptography	115
Monitoring, Vulnerability, and Patch Management.....	118
High Availability, Disaster Recovery, and Physical Protection	121
Incident Response	124
Asset Management and Supply Chain	128
Policy, Audit, E-Discovery, and Training	131
Chapter 4: Implementing Enterprise Cybersecurity	135
Overview	136
Topics.....	137
IT Organization	138
Context	138
Many Possible Reporting Relationships	139
Chief Information Officer (CIO).....	140
Chief Information Security Officer (CISO)	142
IT System Life Cycle	144
Defining Security Policies	148
Defining Security Scopes	149
Context	149
The Eight Types of Security Scopes.....	151
Considerations in Selecting Security Scopes	153

CONTENTS

Identifying Security Scopes	154
Context	154
Security Scopes for the Typical Enterprise	155
Considerations in Selecting Security Scopes	158
Selecting Security Controls	160
Selecting Security Capabilities	163
Selecting Security Technologies	166
Considering Security Effectiveness	168
Chapter 5: Operating Enterprise Cybersecurity	173
Overview	174
Topics	176
Operational Responsibilities	177
High-Level IT and Cybersecurity Processes	180
Context	180
IT Operational Process	181
Risk Management Process	184
Vulnerability Management and Incident Response Process	185
Auditing and Deficiency Tracking Process	190
Operational Processes and Information Systems	193
Context	193
Operational Processes	194
Supporting Information Systems	200
Context	200
Functional Area Operational Objectives	205
Context	205
Chapter 6: Enterprise Cybersecurity and the Cloud	219
Overview	220
Topics	221
Introducing the Cloud	222
Context	222
Five Essential Characteristics	223
Deployment Models	224
Service Models	225

Cloud Protection Challenges	226
Context	226
High-Level Cybersecurity Considerations.....	227
Developer Operations (DevOps) and Developer Security Operations (DevSecOps)	228
Scopes and Account Management	230
Authentication	231
Data Protection and Key Management	232
Logging, Monitoring, and Investigations.....	233
Reliability and Disaster Recovery	234
Scale and Reliability	235
Contracts and Agreements	236
Planning Enterprise Cybersecurity for the Cloud	237
Systems Administration.....	237
Network Security.....	238
Application Security.....	239
Endpoint, Server, and Device Security.....	240
Identity, Authentication, and Access Management	241
Data Protection and Cryptography	242
Monitoring, Vulnerability, and Patch Management	243
High Availability, Disaster Recovery, and Physical Protection.....	244
Incident Response	245
Asset Management and Supply Chain.....	246
Policy, Audit, E-Discovery, and Training	247
Chapter 7: Enterprise Cybersecurity for Mobile and BYOD.....	249
Overview	250
Topics.....	252
Introducing Mobile and BYOD	253
Challenges with Mobile and BYOD	256
Context	256
Legal Agreement for Data Protection	257
Personal Use and Personal Data	258
The Mobile Platform	259
Sensors and Location Awareness.....	260

CONTENTS

Always-On and Always-Connected.....	261
Multi-Factor Authentication.....	262
Mobile Device Management (MDM).....	263
Enterprise Cybersecurity for Mobile and BYOD.....	264
Systems Administration.....	264
Network Security.....	265
Application Security.....	266
Endpoint, Server, and Device Security.....	267
Identity, Authentication, and Access Management.....	268
Data Protection and Cryptography.....	269
Monitoring, Vulnerability, and Patch Management.....	270
High Availability, Disaster Recovery, and Physical Protection.....	271
Incident Response.....	272
Asset Management and Supply Chain.....	273
Policy, Audit, E-Discovery, and Training.....	274
Part III: The Art of Cyberdefense.....	275
Chapter 8: Building an Effective Defense.....	277
Overview.....	278
Topics.....	279
Attacks Are as Easy as 1, 2, 3!.....	280
Enterprise Attack Sequence in Detail.....	281
Context.....	281
Attack Sequence Step 1—Establish Foothold.....	282
Attack Sequence Step 2—Establish Command and Control.....	283
Attack Sequence Step 3—Escalate Privileges.....	284
Attack Sequence Step 4—Move Laterally.....	285
Attack Sequence Step 5—Complete the Mission.....	286
Why Security Fails Against Advanced Attacks.....	287
Context.....	287
Technical Challenge 1—The Failure of Endpoint Security.....	288
Technical Challenge 2—The “Inevitability of ‘the Click’”.....	289
Technical Challenge 3—Systems Administration Hierarchy.....	290
Technical Challenge 4—Escalating Attacks and Defenses.....	291

Business Challenges to Security	292
Context	292
Business Challenge 1—Tension Between Security and Productivity	293
Business Challenge 2—Maximum Allowable Risk	294
Business Challenge 3—Security Effectiveness over Time	295
Business Challenge 4—Security Total Cost of Ownership	296
Philosophy of Effective Defense	297
Context	297
Defense Example 1—Mazes Vs. Minefields	298
Defense Example 2—Disrupt, Detect, Delay, Defeat	300
Defense Example 3—Cybercastles	301
Defense Example 4—Nested Defenses	302
Elements of an Effective Defense	305
Context	305
Effective Defensive Technique 1—Network Segmentation	306
Effective Defensive Technique 2—Strong Authentication	308
Effective Defensive Technique 3—Detection	309
Effective Defensive Technique 4—Incident Response	311
Effective Defensive Technique 5—Resiliency	312
Chapter 9: Responding to Incidents	313
Overview	314
Topics	315
Incident Response Process	316
Context	316
Step 1—Identify the Incident	318
Step 2—Investigate the Incident	319
Step 3—Collect Evidence	322
Step 4—Report the Results	323
Step 5—Contain the Incident	324
Step 6—Repair Gaps or Malfunctions	325
Step 7—Remediate Compromised Accounts, Computers, and Networks	326

CONTENTS

Step 8—Validate Remediation and Strengthen Security Controls	327
Step 9—Report the Conclusion of the Incident.....	328
Step 10—Resume Normal IT Operations	330
Support the Incident Response Process	331
Chapter 10: Managing a Cybersecurity Crisis	333
Overview	334
Topics.....	335
Devastating Cyberattacks and “Falling Off the Cliff”	336
Context	336
The Snowballing Incident	337
Falling Off the Cliff.....	338
Reporting to Senior Enterprise Leadership.....	339
Calling for Help	340
Keeping Calm and Carrying On	341
Context	341
Playing Baseball in a Hailstorm.....	342
Communications Overload.....	343
Decision-Making Under Stress	344
Asks Vs. Needs: Eliciting Accurate Requirements and Guidance	346
The Observe Orient Decide Act (OODA) Loop.....	347
Establishing Operational Tempo	348
Operating in a Crisis Mode	350
Managing the Recovery Process	353
Context	353
Engaging in Cyber Hand-to-Hand Combat.....	354
“Throwing Money at Problems”	355
Identifying Resources and Resource Constraints	356
Building a Resource-Driven Project Plan.....	357
Maximizing Parallelism in Execution	358
Taking Care of People.....	359
Recovering Cybersecurity and IT Capabilities.....	360
Context	360
Building the Bridge While You Cross It.....	361

Preparing to Rebuild and Restore	362
Closing Critical Cybersecurity Gaps.....	364
Establishing Interim IT Capabilities	365
Conducting Prioritized IT Recovery and Cybersecurity Improvements	366
Establishing Full Operating Capabilities for IT and Cybersecurity	367
Cybersecurity Versus IT Restoration.....	368
Maximum Allowable Risk	369
Ending the Crisis	370
Context	370
Resolving the Crisis.....	371
Declaring the Crisis Remediated and Over	372
After-Action Review and Lessons Learned.....	373
Establishing a “New Normal” Culture.....	374
Being Prepared for the Future.....	375
“Disasters happen, and they happen to everyone ... eventually.”	375
Part IV: Enterprise Cyberdefense Assessment.....	377
Chapter 11: Assessing Enterprise Cybersecurity	379
Overview	380
Topics.....	381
Cybersecurity Auditing Methodology	382
Context	382
Cybersecurity Audit Types	387
“Audit First” Design Methodology	390
Context	390
Enterprise Cybersecurity Assessments	395
Context	395
Level 1 Assessment: Focus on Risk Mitigations	398
Level 2 Assessment: Focus on Functional Areas	400
Level 3 Assessment: Focus on Security Capabilities	401
Level 4 Assessment: Focus on Controls, Technologies, and Processes.....	403
Audit Deficiency Management	404

CONTENTS

Chapter 12: Measuring a Cybersecurity Program	407
Overview	408
Topics.....	409
Cybersecurity Measurement	410
Cybersecurity Program Measurement	412
Object Measurement Example	413
Context	413
OM Step 1: Define the question(s) to be answered	414
OM Step 2: Select appropriate objects to measure	415
OM Step 3: For each object, define the object characteristics to measure	416
OM Step 4: For each characteristic, create a value scale.....	417
OM Step 5: Measure each characteristic using the value scales	423
OM Step 6: Calculate the overall cybersecurity program assessment index using object measurement index equation	424
Visualizing Cybersecurity Assessment Scores	425
Cybersecurity Measurement Summary.....	428
Chapter 13: Mapping Against Cybersecurity Frameworks	429
Overview	430
Topics.....	433
Looking at Control Frameworks	434
Clearly Defining “Controls”	436
Mapping Against External Frameworks	438
Context	438
Assessment Audit and Security Scopes	439
IT Systems and Security Controls.....	440
Balancing Prevention with Detection and Response	441
Security Capabilities, Technologies, and Processes	442
Validation Audit and Reporting	444
One Audit, Many Results	445
Context	445
Audit Reporting Mapping.....	446
Deficiency Tracking and Management.....	447

Part V: Enterprise Cybersecurity Program.....	449
Chapter 14: Managing an Enterprise Cybersecurity Program	451
Overview	452
Topics.....	453
Enterprise Cybersecurity Program Management.....	454
Context	454
Step 1: Assess Assets, Threats, and Risks.....	455
Step 2: Identify Security Scopes.....	456
Step 3: Assess Risk Mitigations, Capabilities by Functional Area, and Security Operations.....	458
Step 4: Identify Target Security Levels	460
Step 5: Identify Deficient Areas	461
Step 6: Prioritize Remediation and Improvements	462
Step 7: Resource and Execute Improvements	464
Step 8: Collect Operational Metrics	465
Return to Step 1	466
Assessing Security Status.....	467
Context	467
Cybersecurity Program Steps 3a, 3b, and 3c.....	468
Cybersecurity Program Step 4: Identify Target Security Levels.....	470
Cybersecurity Program Step 5: Identify Deficient Areas.....	472
Cybersecurity Program Step 6: Prioritize Remediation and Improvements.....	473
Analyzing Enterprise Cybersecurity Improvements	474
Context	474
Considering Types of Improvements.....	475
Considering Threat Scenarios.....	476
Examining Cybersecurity Assessment Scores Across Multiple Scopes.....	477
Considering Improvement Opportunities Across Multiple Scopes.....	479
Considering “Bang for the Buck”.....	480
Prioritizing Improvement Projects.....	482
Tracking Cybersecurity Project Results.....	485
Visualizing Cybersecurity Program Assessment Scores.....	485
Measuring Cybersecurity Program Assessment Scores Over Time	486

CONTENTS

Chapter 15: Looking to the Future	487
Overview	488
Generations of Weapons Systems	489
Context	489
Generations of Malware	490
Context	490
Generations of Cyberdefense	491
Context	491
Topics	492
The Power of Enterprise Cybersecurity Architecture	493
Evolution of Cyberattack and Defense	495
Context	495
Before the Internet	496
Generation 1: Hardening the Host	497
Generation 2: Protecting the Network	498
Generation 3: Layered Defense and Active Response	499
Generation 4: Automated Response	500
Generation 5: Biological Defense	501
Cybergenerations Moving Down Market	502
Future Cybersecurity Evolution	503
Evolving Enterprise Cybersecurity over Time	504
Context	504
Enterprise Cybersecurity Implementation Considerations	505
Tailoring Cybersecurity Assessments	506
Evolution of Enterprise Cybersecurity Capabilities	508
Evolution of Enterprise Functional Areas	509
Final Thoughts	510
Part VI: Appendices	513
Appendix A: Sample Cybersecurity Policy	515
Context	516
Topics	518
The Policy	519
Policy Guidance by Functional Area	522

Systems Administration.....	522
Network Security	523
Application Security.....	525
Endpoint, Server, and Device Security.....	526
Identity, Authentication, and Access Management	528
Data Protection and Cryptography	531
Monitoring, Vulnerability, and Patch Management	533
High Availability, Disaster Recovery, and Physical Protection	536
Incident Response	539
Asset Management and Supply Chain	541
Policy, Audit, E-Discovery, and Training	543
Appendix B: Cybersecurity Operational Processes.....	545
Overview	546
Topics.....	547
Policies and Policy Exception Management.....	548
Project and Change Security Reviews	549
Risk Management.....	550
Control Management.....	551
Auditing and Deficiency Tracking.....	552
Asset Inventory and Audit	553
Change Control	554
Configuration Management Database Re-Certification.....	555
Supplier Reviews and Risk Assessments	556
Cyberintrusion Response	557
All-Hazards Emergency Preparedness Exercises.....	558
Vulnerability Scanning, Tracking, and Management.....	559
Patch Management and Deployment.....	560
Security Monitoring.....	561
Password and Key Management.....	562
Account and Access Periodic Re-certification	563
Privileged Account Activity Audit.....	564

Appendix C: Object Measurement	565
Fundamental Principles	566
Topics	570
OM <i>Index</i> Equation	571
General Equation	571
Example Equations	572
OM Steps	573
OM Value Scales	574
Fundamental Principles	574
Example Expert Judgment Value Scales	576
Example Observed Data Value Scales	578
OM Measurement Map	579
Basic Structure	579
Example Enterprise Cybersecurity Program Assessment Measurement Map	580
Expert Judgment OM Example	581
OM Six-Step Methodology	581
Observed Data OM Example	589
OM Six-Step Methodology	589
Other Cybersecurity-Related Measurements	597
Two-Step Measurement Approach	597
Policies and Policy Exception Management	599
Project and Change Security Reviews	600
Risk Management	601
Appendix D: Cybersecurity Sample Assessment	603
Overview	604
Topics	606
Sample Assessment Scope and Methodology	607
Overview	607
Level 1 Assessment: Focus on Risk Mitigations	608
Context	608
Object Measurement Steps	609
What does a Level1 <i>Index</i> = 0.47 or 47% really mean?	617

Level 2 Assessment: Focus on Functional Areas	618
Context	618
Object Measurement Steps	620
What does a Level2_ <i>Index</i> = 0.53 or 53% really mean?	629
Results Visualization and Analysis	630
Level 3 Assessment: Focus on Capabilities	632
Context	632
Object Measurement Steps	634
What does a Level3_ <i>Index</i> = 0.46 or 46% really mean?	656
Results Visualization and Analysis.....	657
Comparing Cybersecurity Assessment Results	658
Using Cybersecurity Assessment Results.....	659
Appendix E: Cybersecurity Capability Value Scales	663
Overview	664
Topics.....	665
Systems Administration	666
Network Security	669
Application Security	673
Endpoint, Server, and Device Security	676
Identity, Authentication, and Access Management.....	680
Data Protection and Cryptography	683
Monitoring, Vulnerability, and Patch Management	686
High Availability, Disaster Recovery, and Physical Protection	690
Incident Response	693
Asset Management and Supply Chain	696
Policy, Audit, E-Discovery, and Training (PAET).....	698
Index.....	701

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.

ABOUT THE AUTHORS

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.

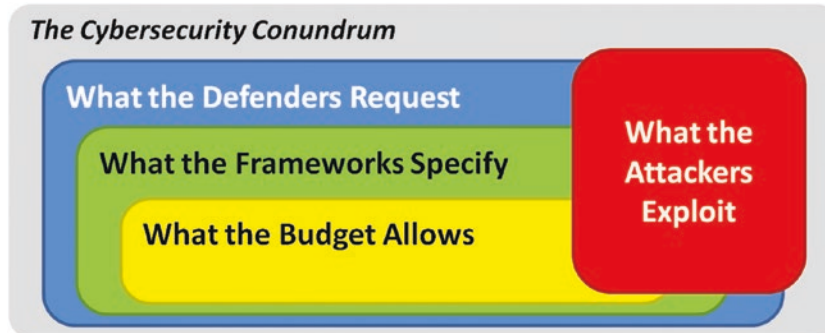


Figure P-1. Even though the cybersecurity conundrum presents significant challenges, implementing a successful cyberdefense program that works against real-world attacks is achievable.

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.

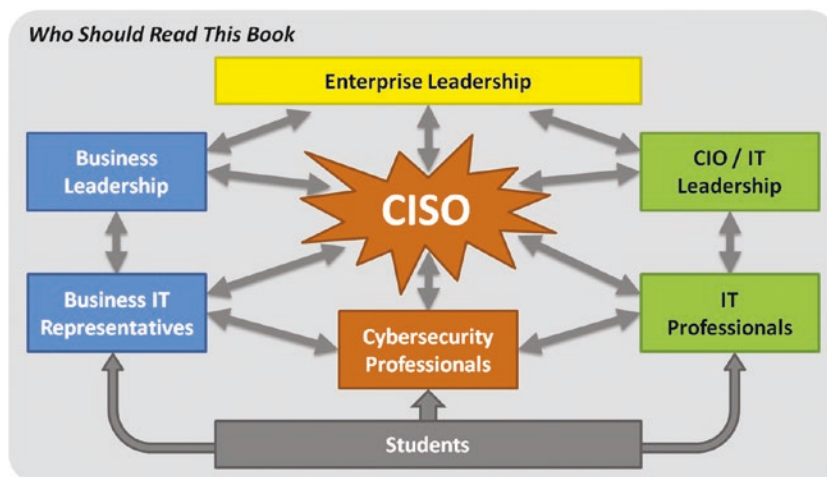


Figure P-2. Successful enterprise cybersecurity is a team sport.

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.

ABOUT THIS STUDY GUIDE

- 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.

ABOUT THIS STUDY GUIDE

- **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.