

THE SECURITY CULTURE PLAYBOOK

AN EXECUTIVE GUIDE TO
REDUCING RISK AND DEVELOPING
YOUR HUMAN DEFENSE LAYER

PERRY CARPENTER
KAI ROER

WILEY

Praise for Perry Carpenter

“The best security behaviors are the ones you never think about, that get ingrained as habits and become part of who you are. Perry’s exploration of security as a cultural force, created by processes and communications but separate from them, is a unique look into precisely that zone of our identity. By stepping away from our biases about what security looks like and focusing on what it practically does, this book invites us forward.”

—Matt Wallaert, Behavioral Scientist and Author of *Start At The End: How to Build Products that Create Change*

“In my time advising companies on how to become more resilient to social engineering, I’ve always touted the importance of building a strong security culture. Perry Carpenter is one of the world’s foremost experts in how to do just that. Security leaders and business executives would be wise to listen to his advice and implement his suggestions.”

—Kevin Mitnick, Principal, Mitnick Security

“Perry has his finger on the pulse of security awareness culture and knows how to bring it to life. His real-world expert advice focuses on what is actionable and most essential for protecting your organization right now.”

—Rachel Tobac, CEO of SocialProof Security and Friendly Hacker

“Perry Carpenter understands that cyber security takes both technology and human accountability. In this excellent new book, he is able to show how both must work together to keep our companies, institutions, and society safe and secure. You should find a number of best practices and insights in this timely book.”

—John R. Childress, Chairman, PYXIS Culture Technologies

“Security culture is fundamental to organizational resilience, efficiency, and success. Perry Carpenter is one of the world’s leading experts in this space, and he communicates his expertise in a way that is engaging and accessible for all.”

—Dr Jessica Barker, co-CEO of Cygenta and Author of *Confident Cyber Security*

“My friend Perry Carpenter has had a long and distinguished infosec career and has had a front row seat to the cybersecurity culture wars from the very beginning. I can’t think of a better guide for organizational executives trying to reduce their inherent risk via an improved internal security culture.”

—Rick Howard, CSO, Chief Analyst, and Senior Fellow at the CyberWire.
Past lives include CSO at Palo Alto Networks, TASC, iDefense GM, Counterpane SOC Director, and the Army’s Computer Emergency Response Team (CERT) Commander

“Perry’s forgotten more on human element security than the rest of us will ever know! Perry understands how our brains work, and how that affects our propensity to be both duped by bad guys and engaged by security awareness content. He’s one of my go-to people in the field.”

—Lisa Plaggemier, Executive Director, National Cybersecurity Alliance

“Security is very much a human issue, and there is no other human I would turn to in order to understand the critical crosshairs of where technology meets culture more than Perry Carpenter. He walks in both realms effectively and, if you want to truly understand how to keep safe in a world without secrets, Perry is your guide and guru. He and Kai have created and curated a playbook that our world needs now more than ever.”

—Michael Leckie, Author of *The Heart of Transformation: Build the Human Capabilities That Change Organizations for Good*

“Too frequently those of us in security think technology first without truly understanding the first priority issue of organizational culture. Culture is integral to organizational success and initiatives. Perry Carpenter’s work in this space is truly second to none. Building on the insights from Transformational Security Awareness, Perry’s work illustrates the vital role of culture with respect to our security programs and risk management.”

—Matt Stamper, Co-Author of the *CISO Desk Reference Guide (Volumes 1 & 2)* CISO & Executive Advisor

Praise for Kai Roer

Kai is a pioneer in security culture awareness, showing CISOs how to drive meaningful changes and move their organizations forward.

—Mirko Zorz, Editor in Chief, Help Net Security

Kai has been pioneering the concepts around security culture for more than a decade, and I've known him for that time as he's built, and sold up, his CLTRE concept. His knowledge on benchmarking a security culture is second to none.

—Dan Raywood, Cybersecurity journalist (former)

I have seen Kai Roer demonstrate his passion and sincere dedication to improving the security culture of organizations for many years. Kai providing guidance for executives to understand their role and responsibility for creating a secure business ecosystem, through using *The Security Culture Playbook*, is a brilliant idea!

—Rebecca Herold, CEO of The Privacy Professor consultancy,
and Privacy & Security Brainiacs SaaS services

I am enthused to learn that Kai Roer has written a new book about security culture.

Kai Roer has taken his many years of cyber experience and combined those with a vested interest in cyber security. By using Kai's Security Culture Framework, I got a tool to address the human and cultural factors in our organization to improve the security maturity.

With clear, everyday examples and analogies to reveal social and cultural triggers that drive human behaviour he guided me through my work. I immediately saw the experience, knowledge, and interpersonal skills that he had for working with people. I most admire Kai for his humor, his determination to reach whatever goals he has put up, and his devotion to throw light on the less technical part of information security.

—Anne-Marie Eklund Löwinder, Founder of Amelsec AB,
inducted into the Internet Hall of Fame, Member of the Royal Swedish
Academy of Engineering Science

There is no one better placed to present expertise related to security culture than Kai. Further, developing a security culture within a given organization is the first line of defence, which makes this book essential reading.

—Raj Samani, McAfee Fellow, Chief Scientist

Kai Is the world leader on security culture helping organizations understand what culture they currently have, what culture they would like to have, and more importantly how to get there.

—Quentyn Taylor, Senior Director – Product, Information Security and Global Incident Response Canon Europe Middle East and Africa

For over a decade, Kai Roer has advised and guided security executives on leading teams and developing culture. His pragmatic approach, informed by psychology and backed by metrics, moves beyond the fluffy platitudes so often found in leadership books. If you are looking for where to begin or wondering what good looks like, Kai Roer’s expertise lights the path.

—J. Wolfgang Goerlich, CISO

I was quite happy living with the knowledge that I had invented the phrase “Security Culture.” Then I met Kai. He had been working on the concept for a couple of years already and went on to become the master of the subject. I am proud to have been on some of that journey with him and have followed and implemented his work at some of the most forward-thinking organizations on the planet.

—Shan Lee, CISO, Wise PLC, ex-Just Eat

Kai is a consummate professional cyber security risk adjudicator and educator; I have known Kai and worked with him for several years, and he is someone I implicitly trust in all settings.

—Bill Hagestad, Author of *21st Century Chinese Cyberwarfare* and several other books on China’s use of computer systems as national strategic weapons. He advises NATO, the US Marine Corps and interfaces with the Chinese People’s Liberation Army (PLA).

There is no such thing as a comprehensive cybersecurity posture without a security culture program. Carpenter and Roer provide executives with all the tools they need to help secure the frontline of defense — the human. With ransomware and novel social engineering techniques on the rise, there has never been a timelier moment for this book — it simply is the must-read cyber book of the year!

—Dr. Lydia Kostopoulos, SVP Emerging Tech Insights

Kai Roer is a person who has been at the forefront of Security Awareness for many years and as such is leading by example. From the early days of his Awareness model to his recent book successes, Kai has proven time and again through his experience in the field implementing his knowledge that he is a true leader in this field.

—Stuart Coulson, Director, HiddenText Ltd

The Security Culture Playbook

Perry Carpenter
Kai Roer

WILEY

Copyright © 2022 by KnowBe4. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

978-1-119-87523-9

978-1-119-87529-1 (ebk.)

978-1-119-87524-6 (ebk.)

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. 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 www.wiley.com/go/permission.

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 Website 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 Website may provide or recommendations it may make. Further, readers should be aware the Internet Websites 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 for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2021952665

Trademarks: WILEY and the Wiley 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. 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.

Cover image: © Getty Images/gremlin

Cover design: Wiley

*For the wonderful community of security awareness,
behavior, and culture professionals around the world. You
are an inspiration.*

*And for my family, Siobhan, Sage, and Aoibheann. Thank
you making life crazy and wonderful!*

—Perry Carpenter

*I dedicate this book to all the amazing first-responders
who continuously keep our society safe and secure without
regard for their own life and health. Thank you!*

—Kai Roer

About the Authors

Perry Carpenter, C|CISO, MSIA, currently serves as Chief Evangelist and Strategy Officer for KnowBe4, the world's most popular security awareness and simulated phishing platform.

Perry has been a recognized thought leader on security awareness and the human factors of security for well over a decade. His broad background makes him uniquely positioned to understand nuances of awareness, behavior, and culture strategies that can be elusive. Perry's security culture influence-related experiences span multiple pivotal roles: from being a general employee receiving awareness training; to being an awareness program manager running complex global programs; to being the primary market analyst advising security leaders about awareness trends, success practices, and vendor platforms; to now helping lead the efforts of the world's largest and most successful security awareness and simulated phishing platform. Perry draws from this experience, along with cutting-edge research in the fields of marketing, communication, behavior science, and organizational culture management

to inform his perspectives and advice for creating security culture influence programs that are transformational.

Before joining KnowBe4, Perry led security awareness, security culture management, and anti-phishing behavior management research at Gartner Research (NYSE:IT), in addition to covering areas of IAM strategy, CISO Program Management mentoring, and Technology Service Provider success strategies. With a long career as a security professional and researcher, Carpenter has broad experience in North America and Europe, providing security consulting and advisory services for many of the world's best-known brands.

Perry's previous book, *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors* (Wiley, 2019) quickly gained a reputation as being the go-to book for security awareness professionals worldwide, and, in 2021, received the honor of being inducted into the Cybersecurity Canon Hall of Fame, a collection of "must-read books for all cybersecurity practitioners—be they from industry, government, or academia—where the content is timeless, genuinely represents an aspect of the community that is true and precise, reflects the highest quality and, if not read, will leave a hole in the cybersecurity professional's education that will make the practitioner incomplete." Institute for Cybersecurity & Digital Trust (2022).

Perry is also the creator and host of the popular *8th Layer Insights* podcast (8thlayerinsights.com), an immersive narrative nonfiction exploration into the intersection of cybersecurity and the human condition. His guest list is a who's who of voices from cybersecurity, behavior sciences, creators, and more.

Perry holds a Master of Science in Information Assurance (MSIA) from Norwich University in Vermont and is a Certified Chief Information Security Officer (CCISO).

You can connect with Perry on LinkedIn at [linkedin.com/in/perrycarpenter](https://www.linkedin.com/in/perrycarpenter).

Kai Roer currently serves as Chief Research Officer for KnowBe4, the world's most popular security awareness and simulated phishing platform.

Kai has been providing actionable advice founded on empirical evidence to public and private organizations around the world since the 1990s. His work over the past decades has focused on helping organizations understand what culture they currently have, what culture they would like to have, and more importantly, how to get there. Kai works with the information security community on a global stage to educate the importance and impact that security culture has.

In 2010, he created the Security Culture Framework (SCF), a framework and methodology to build and maintain security culture. Kai later gifted the SCF to the open-source community, and it evolved into several spin-offs, including the Cybersecurity Culture Framework by The European Union Agency for Cybersecurity (ENISA) in 2015. Kai has authored and co-authored several books on leadership and technology. His popular book *Build a Security Culture* (IT-Governance, 2015) is widely considered as the guiding resource on the topic of security culture.

Before joining KnowBe4, Kai founded the security culture measurement company, CLTRe (pronounced culture), the world's first SaaS-platform built to measure and manage an organization's security culture. This new ability to measure security culture made it possible for organizations worldwide to understand exactly where and how to improve their security. KnowBe4 acquired CLTRe in 2019. After which, Kai built KnowBe4 Research, the research arm of KnowBe4, where he leads a team of researchers dedicated to improving the knowledge and understanding of the human factors that influence security.

Recognized by many as a leading global authority on the topic of security culture, he has received several awards, including the Ron Knode Service Award by the Cloud Security Alliance CSA for his extensive volunteer work in the security community around the world. Thanks to his invaluable contributions to the industry and his unique background that combines leadership, communication,

and technology, Kai is a popular keynote speaker and guest lecturer. He focuses on presenting complex challenges in easy-to-understand language. He is also a frequent guest on podcasts, radio, and TV, where he explains security in ways that resonate with non-security people.

When Kai is not working, he enjoys riding his motorcycles, spending time in the outdoors, and BBQing with his family and friends.

You can connect with Kai at www.linkedin.com/in/kairoer and twitter.com/kairoer.

Acknowledgments

Security culture is a fun and difficult topic to bring to the page. And taking on the challenge certainly comes with its own set of risks and rewards. I'd like to thank all the folks who believed in this project and decided to take the risk. These are people who don't get the benefit of having their names on the cover of this book, but who are absolutely key to any success I or this book will have.

First, this book was a team effort between Kai Roer and me. Even before Kai and I became coworkers at KnowBe4, I was a fan of Kai's work in the field of security culture. It has been an honor to write this book with you!

Second, I need to think the great folks at Wiley Publishing. This is my second book with Wiley, and I'm continually struck by the professionalism, expertise, and compassion that the team brings to each project. Thanks to John Sleeva, Pete Gaughan, and Archana Pragash for helping transform our ramblings into something worthy to be read. And a special thank you to Jim Minatel, my acquisitions editor at Wiley for both this book as well as my previous book,

Transformational Security Awareness. Thanks for believing in both of these projects! You are a true advocate for the community.

I'd also like to thank my wonderful colleagues at KnowBe4. You are a true family, a source of inspiration, and a much needed support system. Any success I have is only because of the support and encouragement you provide. Thanks to Stu Sjouwerman, Kevin Mitnick, Michael Williams, Tiffany Mortimer, Megan Stultz, Kathy Wattman, Greg Kras, Lars Letonoff, Krish Venkatraman, Joanna Huisman, Rosa Smothers, Lydia Kotsiopoulos, Javvad Malik, Roger Grimes, James McQuiggan, Erich Kron, Jacqueline Jayne, Wieringa, Anna Collard, John Just, Winn Schwartz, Kayley Melton, Kendra Irimie, Courtney Orzechowski, Jim Shields, and Rob McCollum. You mean more to me than you'll ever know.

I'd be remiss if I didn't thank my podcast family at The CyberWire for being such an enthusiastic home for my *8th Layer Insights* podcast. You took a chance on me when I had a big vision and no experience, and you've been nothing but supportive. To Peter Kilpe, Jennifer Eiben, Bennett Moe, and Elliott Peltzman. Thanks for your support, advice, and belief in me.

Lastly, I'd like to extend thanks to the security awareness community. There are too many of you to name individually. But, know that this book is for you. You are truly inspiring.

—Perry Carpenter

Sitting here writing in my RV, somewhere in the Norwegian winter landscape, I am grateful for the fact that we live in a world where technology allows us to work from almost anywhere, if we bring our mind, our computer, and some network connectivity along with us. Thank you to all innovators, inventors, and all technologists throughout history—you made this possible!

Writing a book is a huge undertaking. Academics I know liken the process of writing a book with that process of producing a PhD thesis: a lot of dedication, many edits, a fair share of frustration, and a strange combination of solitude when writing and socializing when moving through the editing stages. Thank you, Wiley, and editors Pete Gaughan, Jim Minatel, and Archana Pragash.

Likewise, my team at KnowBe4 Research has been instrumental in the research that supports the writing of this book. Thank you, Anita Eriksen, Thea Ulimoen, and Jacopo Paglia, for your dedication and hard work!

I want to thank my employer KnowBe4 for their continued support of my work and passion: security culture. This book would never have happened without their help both in terms of the time needed for writing, and the sharing of the data and research results used throughout this book. Thank you, KnowBe4 founder and CEO Stu Sjouwerman, and KnowBe4 Chief Marketing Officer Michael Williams for making it possible for me to write this book.

A lot of this book is based on work I have done over my career. Several people have been crucial to me and the process of developing my understanding of security culture, including Roar Thon, Lars Jørgen Kielland Haug, Tone Hoddø Bakås, Jane LeClair, and J. Wolfgang Goerlich. Another instrumental person has been the late Rune Ask, who spent a lot of time taking my early drafts of the Security Culture Framework and adapting them to follow the standard of ISO.

A special mention to my good friend, business associate, co-founder, and brilliantly smart Gregor Petrič who through patience and dedication developed my understanding of the social science underlying much of the work I do. I also want to thank my friend and co-founder Aimee Laycock for her dedication and passion towards the topic of security culture. My son, Leo, the light of my life, and finally, I want to thank my amazing wife, Karolina. We both know that I could not have ventured on this journey without your support!

—Kai Roer

Contents at a Glance

About the Authors	viii
Acknowledgments	xii
Introduction	xxv
PART I: FOUNDATION	1
Chapter 1: <i>You Are Here</i>	3
Chapter 2: Up-leveling the Conversation: Security Culture Is a Board-level Concern	13
Chapter 3: The Foundations of Transformation	27
PART II: EXPLORATION	39
Chapter 4: Just What Is Security Culture, Anyway?	41
Chapter 5: Critical Concepts from the Social Sciences	53

Chapter 6:	The Components of Security Culture	63
Chapter 7:	Interviews with Organizational Culture Experts and Academics	77
PART III:	TRANSFORMATION	95
Chapter 8:	Introducing the Security Culture Framework	97
Chapter 9:	The Secrets to Measuring Security Culture	113
Chapter 10:	How to Influence Culture	129
Chapter 11:	Culture Sticking Points	149
Chapter 12:	Planning and Maturing Your Program	157
Chapter 13:	Quick Tips for Gaining and Maintaining Support	177
Chapter 14:	Interviews with Security Culture Thought Leaders	187
Chapter 15:	Parting Thoughts	207
	Bibliography	213
	Index	217

Contents

About the Authors	viii
Acknowledgments	xii
Introduction	xxv
PART I: FOUNDATION	1
Chapter 1: You Are Here	3
Why All the Buzz?	4
What Is Security Culture, Anyway?	8
A Problem of Definition	9
A Problem of Overconfidence	11
Takeaways	12
Chapter 2: Up-leveling the Conversation: Security Culture Is a Board-level Concern	13
A View from the Top	14
Telling the Human Side of the Story	15
What's the Cost of <i>Not</i> Getting This Right?	16
Cybercriminals Are Doubling Down on Their Attacks Against Your Employees	19

Your People and Security Culture Are at the Center of Everything	20
The Implication	22
Getting It Right	24
Takeaways	25
Chapter 3: The Foundations of Transformation	27
The Core Thesis	29
The Knowledge-Intention-Behavior Gap	29
Three Realities of Security Awareness	31
Program Focus	31
Extending the Discussion	33
Introducing the Security Culture Maturity Model	33
The Security Culture Maturity Model in Brief	35
The S-Curves	36
The Value of the Security Culture Maturity Model	37
You Are Always Either Building Strength or Allowing Atrophy	37
Takeaways	38
PART II: EXPLORATION	39
Chapter 4: Just What Is Security Culture, Anyway?	41
Lessons from Safety Culture	42
A Jumble of Terms	44
Information Security Culture	45
IT Security Culture	45
Cybersecurity Culture	46
Security Culture in the Modern Day	46
Technology Focus	47
Compliance Focus	48
Human-Reality Focus	49
Takeaways	51
Chapter 5: Critical Concepts from the Social Sciences	53
What's the Real Goal—Awareness, Behavior, or Culture?	54
Coming to Terms with Our Irrational Nature	55
We Are Lazy	56

Why Don't We Just Give Up?	60
Security Culture—A Part of Organizational Culture	61
Takeaways	62
Chapter 6: The Components of Security Culture	63
A Problem of Definition	64
The Academic Perspective	64
The Practitioner Perspective	65
Defining Security Culture	66
Security Culture as Dimensions	67
The Seven Dimensions of Security Culture	69
Attitudes	69
Behaviors	69
Cognition	69
Communication	70
Compliance	70
Norms	70
Responsibilities	71
The Security Culture Survey	71
Example Findings from Measuring the Seven Dimensions	72
Normalized Use of Unauthorized Services	73
Confidentiality and Insider Threats	74
Last Thought	74
Takeaways	75
Chapter 7: Interviews with Organizational Culture	
Experts and Academics	77
John R. Childress, PYXIS Culture Technologies Limited	78
Why Is Culture Important?	78
Why Do You Find Culture Interesting?	79
Is There a Specific Definition of Culture That You Find Useful?	79
What Actions Can Be Taken to Direct Cultural Change?	80
Is There a Success or Horror Story You'd Like to Share Related to Culture Change?	81
How Does a Culture Evolve (or How Often?)	82
Professor John McAlaney, Bournemouth University, UK	82
Why Is Culture Important?	83
Why Do You Find Culture Interesting?	83
Is There a Specific Definition of Culture That You Find Useful?	83

What Actions Can Be Taken to Direct Cultural Change? 84

Is There a Success or Horror Story You'd Like to Share
Related to Culture Change? 85

How Does a Culture Evolve (or How Often?) 85

Dejun "Tony" Kong, PhD, Muma College of Business, University
of South Florida 86

Why Is Culture Important? 86

Why Do You Find Culture Interesting? 86

Is There a Specific Definition of Culture That You Find Useful? 87

How Do You Use Metrics to Improve Culture / Measure the
Effectiveness of Cultural Change? 87

Michael Leckie, Silverback Partners, LLC 87

Why Is Culture Important? 88

Why Do You Find Culture Interesting? 89

Is There a Specific Definition of Culture That You Find Useful? 90

How Do You Use Metrics to Improve Culture / Measure the
Effectiveness of Cultural Change? 90

What Actions Can Be Taken to Direct Cultural Change? 91

Is There a Success or Horror Story You'd Like to Share Related to
Culture Change? 93

How Does a Culture Evolve (or How Often?) 93

PART III: TRANSFORMATION 95

Chapter 8: Introducing the Security Culture Framework 97

The Power of Three 99

Step 1: Measure 100

 Know Where You are 101

 Decide Where You Want to Be 102

 Find Your Gap 104

Step 2: Involve 106

 Building Support 106

 Different Audiences 108

Step 3: Engage 109

Rinse and Repeat 111

Benefits of Using the Security Culture Framework 111

Takeaways 112

Chapter 9: The Secrets to Measuring Security Culture	113
Connecting Awareness, Behavior, and Culture	115
How Can You Measure the Unseen?	116
Using Existing Data	116
The Right Way to Use Data	119
Methods of Measuring Culture	119
Observation	120
Experimentation	121
Interrogation (Surveys and Interviews)	121
A/B Testing	122
Multiple Metrics, Single Score	124
Trends	125
A Note Regarding Completion Rates	127
Takeaways	128
Chapter 10: How to Influence Culture	129
Resistance to Change	130
Be Proactive	131
The Complexity of Culture	133
Using the Seven Dimensions to Influence Your Security Culture	134
Attitudes	134
Behaviors	136
Cognition	138
Communication	140
Compliance	141
Norms	143
Responsibilities	144
How Do You Know Which Dimension to Target?	146
Takeaways	147
Chapter 11: Culture Sticking Points	149
Does Culture Change Have to Be Difficult?	150
Using Norms Is a Double-Edged Sword	151
Failing to Plan Is Planning to Fail	152
If You Try to Work Against Human Nature, You Will Fail	153
Not Seeing the Culture You Are Embedded In	155
Takeaways	156

Chapter 12: Planning and Maturing Your Program	157
Taking Stock of What We've Covered	158
View Your Culture Through Your Employees' Eyes	159
Culture Carriers	160
Building and Modeling Maturity	161
Exploring the Data	162
Culture Maturity Indicators	162
Level 1: Basic Compliance	165
Level 2: Security Awareness Foundation	165
Level 3: Programmatic Security Awareness & Behavior	166
Level 4: Security Behavior Management	167
Level 5: Sustainable Security Culture	168
There Are Stories in the Data	170
A Seat at the Table	174
Takeaways	175
Chapter 13: Quick Tips for Gaining and Maintaining Support	177
You Are a Guide	178
Sell by Using Stories	179
Lead with Empathy, Know Your Audience	180
Set Expectations	184
Takeaways	185
Chapter 14: Interviews with Security Culture Thought Leaders	187
Alexandra Panaretos, Ernst & Young	188
Why Is Culture Important?	188
Why Do You Find Culture Interesting?	189
Is There a Success or Horror Story You'd Like to Share Related to Culture Change?	190
Dr. Jessica Barker, Cygenta	193
Why Is Security Culture Important?	193
Why Do You Find Culture Interesting?	194
What Actions Can Be Taken to Direct Cultural Change?	194
What Is Your Most Interesting Experience with Culture?	195
Kathryn Tyrpak, Jaguar Land Rover	195
Why Is Culture Important?	195
Why Do You Find Culture Interesting?	196
Is There a Specific Definition of Culture That You Find Useful?	196

How Do You Use Metrics to Improve Culture / Measure the Effectiveness of Cultural Change?	196
What Actions Can Be Taken to Direct Cultural Change?	197
Lauren Zink, Boeing	197
Why Is Culture Important?	198
Why Do You Find Culture Interesting?	198
Is There a Specific Definition of Culture That You Find Useful?	199
How Do You Use Metrics to Improve Culture / Measure the Effectiveness of Cultural Change?	199
Mark Majewski, Rock Central	200
Why Is Culture Important?	200
Why Do You Find Culture Interesting?	200
Is There a Specific Definition of Culture That You Find Useful?	201
How Do You Use Metrics to Improve Culture / Measure the Effectiveness of Cultural Change?	201
What Actions Can Be Taken to Direct Cultural Change?	201
Is There a Success or Horror Story You'd Like to Share Related to Culture Change?	202
How Does a Culture Evolve (or How Often)?	202
Mo Amin, moamin.com	203
Why Is Culture Important?	203
Why Do You Find Culture Interesting?	203
Is There a Specific Definition of Culture That You Find Useful?	203
How Do You Use Metrics to Improve Culture / Measure the Effectiveness of Cultural Change?	203
What Actions Can Be Taken to Direct Cultural Change?	204
Is There a Success or Horror Story You'd Like to Share Related to Culture Change?	204
How Does a Culture Evolve (or How Often)?	205
Chapter 15: Parting Thoughts	207
Engage the Community	208
Be a Lifelong Learner	209
Be a Realistic Optimist	210
Conclusion	211
Bibliography	213
Index	217