Foreword by
KEVIN MITNICK

TRANSFORMATIONAL SECURITY AWARENESS

What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors

PERRY CARPENTER

WILEY

Transformational Security Awareness

Transformational Security Awareness

What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors

Perry Carpenter

WILEY

Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-119-56634-2
ISBN: 978-1-119-56637-3 (ebk.)
ISBN: 978-1-119-56635-9 (ebk.)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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 website may provide or recommendations it may make. Further, readers should be aware that 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 please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States 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: 2019933733

For Siobhan, Sage, and Lily: the best reasons imaginable to help build a more secure planet. Oh - and thanks for putting-up with all the puns . . .

About the Author

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 strategy that can be elusive. Perry's security awareness-related experiences spans 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 awareness 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 holds a Master of Science in Information Assurance (MSIA) from Norwich University in Vermont and is a Certified Chief Information Security Officer (C|CISO).

You can connect with Perry on LinkedIn at: `https://linkedin.com/in/perrycarpenter`.

About the Technical Editor

Matt Stamper, CISA, CISM, CIPP/US, ITIL, brings a broad, multi-disciplinary understanding of cybersecurity best practices. His diverse domain knowledge spans IT service management (ITSM), cybersecurity, cloud services, control design and assessment (Sarbanes-Oxley, HIPAA-HITECH), privacy (GDPR, CCPA), enterprise risk management (ERM), and IT risk management (ITRM).

Matt excels at conveying complex cybersecurity and IT concepts to boards of directors, executive management, as well as professional service providers. His executive and board-level experience with managed services, cybersecurity, data centers, networks services, and ITSM provide a unique perspective on the fast-changing world of enterprise IT, IoT, and cloud services.

Stamper was a Research Director within the Security and Risk Management Practice at Gartner (NYSE:IT). During his time at Gartner, Stamper met with CISOs and CIOs across the globe to address cybersecurity program development, security incident response, and other security topics. Matt was the co-author on the Magic Quadrant for IT Risk Management Solutions and wrote research on incident response and covered breach and attack simulation technologies. Matt is also the co-author of the CISO Desk Reference Guide (Volumes 1 & 2).

You can connect with Matt on LinkedIn at: `https://www.linkedin.com/in/stamper/`

Credits

Associate Publisher
Jim Minatel

Editorial Manager
Pete Gaughan

Production Manager
Kathleen Wisor

Project Editor
Tom Dinse

Production Editor
Athiyappan Lalith Kumar

Technical Editor
Matt Stamper

Copy Editor
Kim Wimpsett

Proofreader
Evelyn Wellborn

Indexer
Johnna VanHoose Dinse

Cover Designer
Wiley

Cover Image
© wildpixel/iStockphoto

Acknowledgments

Wow! Writing a book is such a big process; draining at times, and life-giving at others. During the writing of this book I had times of intense focus and productivity when it felt like words and information were gleefully flying from my fingertips to my keyboard and onto my screen, sitting there virtually smiling back at me. And there were other times when, frankly, I felt like finding a box of toothpicks and stabbing the entire contents of the box, toothpick by toothpick, into my eyes just to make it end.

Ok . . . that's a bit of an exaggeration. But you wanna' know what's not an exaggeration? Sure you do. So, I say this in all seriousness: Though my name adorns the wonderfully designed cover of this book, it is only able to do so because of a list of countless other names. The names of people who have provided me with so much help and encouragement throughout my life and career.

I'll start with the most important group in my life: my family. To my amazing wife, Siobhan: Thank you for always believing in me; for dealing with my craziness; and for helping me become a better version of myself, every day. You have the biggest heart of anyone I know. I'm so lucky to call you my bride and my friend. To my kids, Sage and Lily: I love you more than words can express. You make me prouder than you'll ever know.

Thanks to my mom and dad for always encouraging me to be multidisciplinary in my thinking and skills development. That multidisciplinary thinking is at the core of this book.

There are so many great people who've helped me throughout my career; many of whom I've never thanked. First and foremost are George Brooks and David Newton, two managers who took chances hiring a young, relatively inexperienced guy who dropped out of law school because he wanted to plunge into the wonderful world of software development. If not for your faith in me, the chances you took, and the responsibilities that you gave me nearly 20 years ago, this book would certainly not exist.

By far the two people who shaped the way that I've approached my security career more than anyone else are Greg Schaffer and Whitney Bell. I have no idea how you both put up with me, but you did. I think of your patience, guidance, trust, and mentorship often. And I hope that, in some little way each day, I'm able to reflect your values back into the world.

During my time at Gartner, I had the privilege to make great friends, have wonderful managers, and work with some of the brightest folks on the planet. To Ray Wagner, Andrew Walls, Ash Ahuja, Michele Caminos, Joanna Huisman, Tom Scholtz, Jeffrey Wheatman, Paul Proctor, Neil Wynne, Neil MacDonald, Ant Allan, Gregg Kreizman, Earl Perkins, Terry Hicks, and countless more, thank you for your friendship, guidance, and mentorship.

For those who helped lead awareness efforts with me at my previous employers. Thank you! Roy Eggensperger for being my partner in crime way back in the 2006-ish timeframe and wanting to help move our awareness program forward in new, interesting, and crazy ways. And to Amber Styles-Emberson, Vladimir Skoric, and Kym Patterson, thank you for your tireless efforts in creating and running an innovative large-scale program under enormous internal pressure and external scrutiny.

I have so many great coworkers at KnowBe4 that I work with every day and who encouraged me to tackle this project. First and foremost, I need to thank Roger Grimes. Thank you for believing that I can not only have a book proposal accepted, but also believing that I can deliver on my mission for the book.

To Stu Sjouwerman for giving me the go-ahead to effectively split my attention for six months and for reading and providing encouraging feedback on my earliest drafts. You are an amazing CEO, leader, mentor, and friend.

Thanks to Kevin Mitnick for your friendship and encouragement. I learn something interesting and fun (and often, scary) every time we get together.

And, thank you to Kathy Wattman, Kendra Irimie, Mary Owen, Laurie Haynes, Roger Grimes, Erich Kron, Amanda Tarantino, Rob Henley, Greg Kras, and Alin Irimie. I could not ask for a better or more supportive group of folks to work with daily. Each of you are amazing and inspiring in so many ways.

Thanks to Jim Shields, Rob McCollum, Richard Leverton and all the amazing people at Twist & Shout for being the creative force and production expertise behind *The Inside Man*. This video series was a dream realized for me and was probably the most fun project I've worked on in my career.

Believe it or not, even though I work for a vendor serving the security awareness market, I've received a ton of encouragement and support from other vendors in this space as I let them know about this book. Special thanks to Lance Spitzner (SANS Security Awareness), Lisa Plaggemier (InfoSec Institute), Tom Pendergast (MediaPro), and Masha Sedova (Elevate Security). Your faith in my handling of the material and encouragement throughout this project mean more to me than you can possibly know.

Thanks to Beth Beerman and Kathy Michael of the International Association of Security Awareness Professionals (IASAP) for your support and for sending some of your members my way to be interviewed. Having the voices of practitioners as part of this book helps ensure that the concepts are connected to how they can be implemented in the real world.

A HUGE thank you to BJ Fogg and Stephanie Weldy for reviewing the sections on the Fogg Behavior Model and for working through several iterations of text and graphics to ensure that I've captured the essence of the model faithfully and that it is applied accurately. Your support and input shine through and will make the behavior-related aspects of this book have the gravitas they deserve.

This book wouldn't have been possible without the constant help and encouragement provided by the folks at Wiley Publishing. Jim Minatel, Tom Dinse: you both made this process as painless as possible. In everything from first-timer, newbie questions to schedule issues, to strange requests about wording, graphics, and more, you were constantly encouraging and supporting. Thank you! Thank you also, to Athiyappan Lalith Kumar for being a thorough and thoughtful editor. Additionally, there is an amazing team of professionals who believe that the printed word is still incredibly powerful. These people do all the heavy lifting to ensure that a project like this is successful. Thank you! It was fantastic working with you all!

And, finally, thanks to my technical editor and reviewer, Matt Stamper. I'm so glad you were able to lend your CISO and executive strategy lens to this work. I appreciate all the thoughtful comments, suggested edits, points to ponder, and encouragement that you lent along the way. This project was a great excuse to work together and to get to know you better.

-Perry Carpenter

Contents at a Glance

Contents

Foreword

Perry Carpenter is a highly respected cybersecurity guru who I've gotten to know over the last two years. He has 15+ years of experience in the field both as a practitioner and as an analyst. He's sharp, is incredibly analytical, has a knack for psychology, and is a prolific writer. I first met Perry when he started working at KnowBe4, but I'd heard of him when he was an analyst at Gartner through KnowBe4's CEO Stu Sjouwerman. Perry and I always play off of one another on webinars that we put on together for KnowBe4. We have a natural chemistry that is sometimes hard to find. A big reason for that natural chemistry is one of the first things that drew me to him—our mutual love of magic. We both have such a fascination with it that we took turns showing each other magic tricks one day.

Social engineering threats have been around since before I was born. Con artists continue to get better. That's a big reason why I look at security awareness as an absolute necessity—because humans can be easily influenced to reveal confidential information or to perform actions through manipulation and deception. Regardless of what the software does, humans can be tricked to do whatever another human wants. There's no software in the world that can protect a system against a pretext. People must realize that technology alone won't protect them. That's why it's crucial to implement entertaining, relevant, and informative security training to make it matter to employees personally (appeal to self-interest), which helps change behavior.

Perry has put together a comprehensive book about security awareness programs that every security professional should read. It covers a variety of topics related to security awareness including the psychology of the behaviors behind getting someone to perform a certain act or care about a certain topic, the use of marketing and communications tactics to enhance security awareness training, leveraging social pressures to change culture, and more. He's also added a compilation of voices from the cybersecurity industry who provide their advice about how to put on your best security awareness training.

Not only does Perry address the "how" behind putting together a comprehensive and effective security awareness training program, he addresses the ever important "why." Why should people care about it? Why would it appeal to him/her personally? He even breaks it down to simplify why you should have a security awareness training program in the first place. Knowing the ultimate purpose and goal of your security awareness program is important because it correlates directly to the impact of your program.

One thing that I particularly enjoyed about his book was that he talked in detail about the importance of repetition when it comes to effectively getting a message across, and then he proceeds to summarize and repeat the most important points at the end of each chapter in the book. Perry also uses a line throughout the book that I'm a big fan of: "Just because I'm *aware* doesn't mean I *care*." Keep that in mind as you develop your security awareness program. Plan for it and work with human nature rather than against it to make your program more effective and to go beyond mere awareness. When we connect with people on an emotional level, the chance of them actually caring increases dramatically. Your ultimate goal should be to change end-user behavior and to shape the organization's overall security culture.

We can't argue that the world is in desperate need of better equipped security awareness leaders. And the human element is the most important one when it comes to your cybersecurity program. Beyond technology, beyond software, people are truly your last line of defense. At the end of the day, it all comes down to people. Perry has a way of masterfully exploring how people think and why they act the way they do. This is a fascinating read and, once again, something I'd recommend to everyone in the cybersecurity field.

—Kevin Mitnick

Introduction

I have a confession to make. This may sound strange, but pondering human thought and behavior is one of my favorite things to do. I think it's always been that way for me. I've wanted to know what makes people tick. Because of that, I've gone down a few interesting roads of study, from music, to religious studies, to magic and misdirection, to social engineering, to training as a street hypnotist and theatrical mind-reader, to taking classes in pickpocketing, to learning the ins and outs of public speaking and influence tactics, to graphic design, and more.

In all of this, I think I've actually been trying to understand why I do the things that I do and think the things that I think. You see, I've always felt a bit different. And that difference was confirmed to me late in life when I was diagnosed with Asperger's syndrome (a neurological difference also known as autism spectrum disorder, or ASD). In many aspects of life, this neurodiversity has served me well. I see the world in a different way. And that off-centered view of things has helped me find solutions or phrase answers in ways that can sometimes elude others. And, often, I'm sure that my way of approaching things has resonated not because it is better or more insightful; rather, it can resonate because it is quirky enough to cut through someone's pre-established filters.

In other areas of life, the social areas, I often felt (and sometime still feel) like an alien or a social anthropologist seeking to better understand the strange and wonderful inhabitants of this world. That *seeking to understand* is something that I still do every day. So, pondering human thought (psychology), our behavior (behavior science), and group dynamics (culture) is ceaselessly interesting and fun. The best part of it (professionally) is that I've had the opportunity in my career to make this quest part of the mandate for my daily job.

The Security Awareness Connection

The various roles throughout my professional life have offered me a unique vantage point when it comes to security awareness programs and to the security awareness market. I've seen security awareness from virtually every conceivable angle.

- I've been the recipient of security awareness training at former employers.
- I've designed and implemented security awareness programs at multiple Fortune 500 companies.
- I've served as the Gartner analyst covering the security awareness market, authoring the Magic Quadrant for the space, advising vendors, and helping security awareness program managers design their programs.
- And now, I help shape the awareness market and seek to serve security awareness leaders around the world by working within the security awareness vendor community.

Over the 15 or so years that I've been directly involved in building my own programs, advising security leaders and vendors, or helping shape the future of KnowBe4, I've learned a thing or two about what makes a security awareness program viable and scalable for long-term success. I've seen what does and doesn't work. And I've helped to build real, functional, security awareness programs that have shaped the behavior of employees as well as molding the way that organizations perceive and value security within their broader culture. Isn't that our goal? I'm pretty sure you agree. After all, if that's not what you are hoping to achieve, you probably wouldn't be reading this.

I'm resisting the urge to summarize the entire book for you right now. But, as I do that, there are a few things that I can't help but allow to leak forward and spill onto this page. Specifically, I want to let you in on the main thesis of this book. It's this: the concept of "security awareness" can suffer from a fatal flaw, what I call the *knowledge-intention-behavior gap*. Just because your people are *aware* of something doesn't mean that they will *care*. And, even if they *care* and *intend* to do the right thing, a whole host of situations and contexts can interfere with the follow-through (the desired *behavior*). So, there is a gap between *knowledge* and *intention*. And there is a gap between *intention* and *behavior*.

A *transformational* security awareness program proactively accounts for the *knowledge-intention-behavior gap*. It does so by working with, rather than against, human nature. And it does so by setting an intentional, eyes-open, focus on the idiosyncrasies of human nature, human behavior, human thought and reasoning, social dynamics, the power of emotion, and more. A transformational security awareness program will allow these realities to define the program strategy rather than just tossing out the next security video or dragging everyone through the doldrum of the next annual PowerPoint fest.

Thinking Forward

I was very intentional about the cover image for this book. Take another look at it now. When we think about the concept of transformation, it's easy to think about a caterpillar's transformation into butterfly. But all too often, we think about the butterfly emerging from the cocoon. That's great—but it's the *end* of the story. Notice, however, in the cover photo, you see the caterpillar casting the *shadow* of a butterfly. It's about the future potential of what exists in the now.

This book is about helping you see the potential of what is possible and then helping you plan practical ways to move toward that transformational outcome. So, in the same way that you can look at a caterpillar and imagine the future butterfly, I want to you imagine. Imagine yourself, your program, your people, and your organization a year from now: *transformed*.

Let the Fun Begin

Let's make this a conversation. I'd love to know your thoughts as you progress through the book. Keep me up-to-date on any transformational stories you have. Or, let me know if I can help with anything.

Lastly, if you enjoy this book and think it's helpful, recommend it to others, write a review, and buy copies to give to all your friends, family, and co-workers this holiday season. OK, that last part was somewhat in jest. But I do sincerely hope to hear from you.

You can connect with me on LinkedIn (`/in/perrycarpenter`), on Twitter (`@perrycarpenter`), or on the Web (`https://TheSecurityAwarenessGuy.com`).

Perry Carpenter
March 2019

The Case for Transformation

In This Part

Chapter 1: You Know Why. . .

Chapter 2: Choosing a Transformational Approach