



PEOPLE- CENTRIC Security

Transforming Your Enterprise Security Culture



Lance Hayden, PhD

Foreword by Lance Spitzner, SANS

People-Centric Security

Transforming Your Enterprise
Security Culture

Lance Hayden



New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

Copyright © 2016 by McGraw-Hill Education. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN: 978-0-07-184679-0

MHID: 0-07-184679-4

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-184677-6,
MHID: 0-07-184677-8.

eBook conversion by codeMantra
Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." MCGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

To Jayne and Wyatt, because everything.

About the Author

Dr. Lance Hayden is a managing director in the Technology Advisory Practice of BRG, an international strategy and research firm. Dr. Hayden's security career spans 25 years across the public, private, and academic sectors. His interest in human security behaviors and culture began while a HUMINT operations officer with the Central Intelligence Agency, and continued in security roles at companies including KPMG, FedEx, and Cisco. Dr. Hayden provides expert advice and consulting on information security strategy, measurement, and culture to companies and governments around the globe. In addition to *People-Centric Security*, he is the author of *IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data*, also from McGraw-Hill Education. Lance received his PhD in information science from the University of Texas, where he also teaches courses on security, privacy, and the intelligence community. He lives in Austin.

About the Technical Editor

David Phillips has been protecting clients' IT systems for over 20 years, including technical mitigation, information security risk programs, IT network security architecture, and regulatory compliance. David developed a growing professional service business inside a multinational networking corporation focused on cybersecurity, protecting clients' intellectual property and customer data, and securing networks to allow for resilient IT infrastructure in the face of cyberattacks. His clients have included multibillion-dollar businesses in the retail, finance, manufacturing, energy, and healthcare verticals. David has worked with global enterprises to measure and mature their security capabilities across people, process, and technology, spanning levels from technology management to security awareness and security cultural transformation. David lives outside of Austin, Texas.

Contents at a Glance

Part I	Understanding Your Security Culture	
Chapter 1	Information Security: Adventures in Culture Hacking	3
Chapter 2	Strategy for Breakfast: The Hidden Power of Security Culture	19
Chapter 3	Organizational Culture: A Primer	39
Chapter 4	Cultural Threats and Risks	59
Part II	Measuring Your Security Culture	
Chapter 5	The Competing Security Cultures Framework	81
Chapter 6	The Security Culture Diagnostic Survey (SCDS)	115
Chapter 7	Creating Culture Maps with the Security Culture Diagnostic Survey . . .	139
Chapter 8	Implementing a Successful Security Culture Diagnostic Project	159
Part III	Transforming Your Security Culture	
Chapter 9	From Diagnosis to Transformation: Implementing People-Centric Security	189
Chapter 10	Security FORCE: A Behavioral Model for People-Centric Security	201
Chapter 11	The Security Value of Failure	219
Chapter 12	The Security Value of Operations	239
Chapter 13	The Security Value of Resilience	263
Chapter 14	The Security Value of Complexity	285

Chapter 15	The Security Value of Expertise	309
Chapter 16	Behavior and Culture: Mastering People-Centric Security	333
Chapter 17	Leadership, Power, and Influence in People-Centric Security	357
Chapter 18	Securing a People-Centric Future	369
	Index	381

Contents

Foreword	xvii
Acknowledgments	xviii
Introduction	xix

Part I Understanding Your Security Culture

Chapter 1	Information Security: Adventures in Culture Hacking	3
	Burnt Bacon	4
	Safe and Not Secure	6
	What Were You Thinking?	6
	Culture Hacking	7
	Software of the Mind	8
	A Brief History of Culture Hacking	9
	Security Culture: Hack or Be Hacked	10
	Who's Hacking Your Security Culture?	11
	Security, Hack Thyself	12
	Culture Hacks: The Good	14
	Culture Hacks: The Bad	15
	Culture Hacks: The Ugly	16
	Security Is People!	17
	Further Reading	17
Chapter 2	Strategy for Breakfast: The Hidden Power of Security Culture	19
	Why Security Fails	20
	We Start with a Design	20
	Warning Signs	22
	Doing More with Less	23
	Who Moved My Fence?	24
	Look Out Below!	27
	Getting the Drift	27

	The Opposite of Monoculture	28
	Cultural Traits in Information Security	30
	Competing Values and Security Threats	34
	The Change Agents of Security Culture	35
	The C-Suite	35
	Security Awareness Teams	36
	Security Researchers	36
	Security Practitioners	37
	Making Security Cultural	38
	Further Reading	38
Chapter 3	Organizational Culture: A Primer	39
	The Field of Organizational Culture	41
	Origins	41
	Outcomes	42
	The Culture Iceberg	43
	Hidden Aspects	44
	People Powered	46
	The Organizational Cultural/Organizational Performance Link	47
	Assessing and Measuring Culture	49
	Qualitative vs. Quantitative Measurement of Culture	49
	Qualitative Measures and Techniques	50
	Culture by the Numbers	51
	Challenges of Cultural Transformation	53
	There's No One Right Way to Change Culture	54
	You Have to Include Everybody	54
	You Have to Build Consensus	54
	You Have to Evaluate the Outcomes	55
	You Have to Have Good Leadership	56
	An Ocean of Research	57
	Further Reading	57
Chapter 4	Cultural Threats and Risks	59
	Cultural Threat Modeling	60
	Covert Processes and Cultural Risk	61
	Getting to Know PEPL	62
	Political Threats	64
	Emotional Threats	66

Psychological Threats	68
Logistical Threats	72
Cultural Competition as a Source of Risk	73
Sizing Up the Competition	74
Further Reading	77

Part II Measuring Your Security Culture

Chapter 5	The Competing Security Cultures Framework	81
	Measuring Security Culture	82
	Quantitative Data and Analysis	83
	Qualitative Data and Analysis	87
	Combining the Qualitative and Quantitative	88
	Other Ways of Describing Culture	91
	The Competing Security Cultures Framework	94
	Origins of the CSCF in Competing Values Research	94
	Adapting the Competing Values Framework to Security	96
	The CSCF Quadrants	99
	Overlapping and Competing Values	100
	Limitations of the Framework	101
	Why Not Just Use the Competing Values Framework?	102
	Security Culture Benefits From a Targeted Approach	102
	Not Everything in the Competing Values Framework Translates Well	103
	Organizational Security Cultures	104
	Process Culture	104
	Compliance Culture	106
	Autonomy Culture	109
	Trust Culture	112
	Further Reading	114
Chapter 6	The Security Culture Diagnostic Survey (SCDS)	115
	SCDS Format and Structure	117
	How Surveys Work	117
	Questions in the SCDS	118
	SCDS Scoring Methodology	125
	Scoring the SCDS Results	126

	Security Culture Diagnostic Strategies: Case Studies	128
	ABLE Manufacturing: Measuring an Existing Security Culture	128
	CHARLIE Systems, Inc.: Comparing Security Cultures of Two Organizations	133
	DOG: Comparing Existing to Desired Security Culture	135
Chapter 7	Creating Culture Maps with the Security Culture Diagnostic Survey	139
	Security Culture Maps	141
	Mapping Security Culture Using the CSCF	141
	Composition of a SCDS-based Culture Map	143
	Other Techniques for Mapping Security Culture	146
	“When Should I Use Each Type of Map?”	148
	Mapping Specific Values and Activities	149
	Interpreting and Comparing Culture	150
	Interpreting SCDS Results	151
	Comparing Cultures	156
Chapter 8	Implementing a Successful Security Culture Diagnostic Project	159
	Getting Buy-in for the Security Culture Diagnostic Project	160
	Direct Benefits of Security Culture Improvement	160
	Estimating the Financial Impact of Security Culture	162
	Case Study: FOXTROT Integrators, Inc.	164
	Executing a Security Culture Diagnostic Project	170
	1. Setting Up the Project	171
	2. Collecting Data	175
	3. Analyzing Responses	180
	4. Interpreting Culture and Communicating Results	181
	From Measurement to Transformation	185
	Further Reading	185

Part III Transforming Your Security Culture

Chapter 9	From Diagnosis to Transformation: Implementing People-Centric Security	189
	Diagnosis and Transformation: One Coin, Two Sides	190
	The CSCF as a Framework for Understanding	190
	What Is the Framework for Transformation?	191
	Behavioral Models for Security Culture Transformation	192
	Compliance and Control Regimes	192
	Security Process Improvement	194

	Technology and Automation Approaches	196
	Security Needs More Options	198
	Further Reading	199
Chapter 10	Security FORCE: A Behavioral Model for People-Centric Security	201
	Origins of Security FORCE	203
	HRO Research	204
	HROs in Information Security	206
	Introducing the Security FORCE Behavioral Model	208
	Five Core Values of Security FORCE	209
	Security FORCE Value Behaviors and Metrics	211
	Security FORCE Value Behaviors	212
	Security FORCE Value Metrics	212
	The Culture—Behavior Link in HRSPs	215
	Further Reading	217
Chapter 11	The Security Value of Failure	219
	What Is the Security Value of Failure?	220
	“Failure Is Not an Option”	220
	Reevaluating Failure	221
	Embracing Failure	223
	Fail Small, Fail Fast, Fail Often	224
	Failure Key Value Behaviors	226
	Anticipate Failures	227
	Seek Out Problems	227
	Reward Problem Reporting	228
	Share Information About Failures	229
	Learn from Mistakes	230
	Assessing Your Failure Value Behaviors	232
	The Security FORCE Survey	232
	The Security FORCE Metrics	234
	Improving Your Failure Value Behaviors	237
	Embed the Security Value of Failure into People	237
	Reeducate People on What It Means to Fail	237
	Set Leadership Examples	238
	Open Up Communication	238
	Further Reading	238

Chapter 12	The Security Value of Operations	239
	What Is the Security Value of Operations?	240
	Operational Power	241
	Sensitivity to Operations	241
	Expectations and Reality	243
	Operations Key Value Behaviors	244
	Keep Your Eyes Open	245
	Form a Bigger Picture	246
	“Listen” to the System	247
	Test Expectations Against Reality	249
	Share Operational Assessments	252
	Assessing Your Operations Value Behaviors	255
	Scoring the Operations Value Behavior Survey	255
	FORCE Value Metrics for Operations	256
	Improving Your Operations Value Behaviors	259
	Embed Operations Value into the Security Program	259
	Think More Like Scientists	260
	Embrace the “Sharing Economy”	260
	Lighten Up a Bit	261
	Further Reading	261
Chapter 13	The Security Value of Resilience	263
	What Is the Security Value of Resilience?	264
	When Bad Things Happen (to Good Organizations)	264
	Rolling with the Punches	266
	Imagining Failures and Disasters	267
	Resilience Key Value Behaviors	270
	Overtrain People	270
	Create “Skill Benches”	272
	Actively Share Expertise	273
	Encourage Stretch Goals	274
	Practice Failing	275
	Assessing Your Resilience Value Behaviors	278
	Scoring the Resilience Value Behavior Survey	278
	FORCE Value Metrics for Resilience	279

	Improving Your Resilience Value Behaviors	281
	Embed Resilience Value into the Security Program	282
	“A Security Incident? I Want In!”	282
	Make Security Incidents Mundane	283
	Further Reading	283
Chapter 14	The Security Value of Complexity	285
	What Is the Security Value of Complexity?	286
	Dumbing It Down	287
	Growing Uncertainty	288
	Ignorance Is Risk	290
	Complexity Key Value Behaviors	294
	Don’t Oversimplify	295
	Formalize Your Assumptions	296
	Covet Empirical Evidence	297
	Share the Doubt	298
	Make Every Model Better	299
	Assessing Your Complexity Value Behaviors	300
	Scoring the Complexity Value Behavior Survey	301
	FORCE Value Metrics for Complexity	302
	Improving Your Complexity Value Behaviors	304
	Embed Complexity Value into the Security Program	305
	Think Bigger	306
	Accept What We Already Know	306
	Further Reading	307
Chapter 15	The Security Value of Expertise	309
	What Is the Security Value of Expertise?	311
	Filter Your Water, Not Your Information	311
	Structural Authority vs. Structural Knowledge	312
	Waiting for the Big One	315
	Expertise Key Value Behaviors	317
	Ask the Experts	318
	Suppress the Egos	319
	Allow Authority to Migrate	320
	Share Credibility	321
	Reward Calls to Action and Cries for Help	322

	Assessing Your Expertise Value Behaviors	324
	Scoring the Expertise Value Behavior Survey	325
	FORCE Value Metrics for Expertise	326
	Improving Your Expertise Value Behaviors	328
	Embed Expertise Value into the Security Program	329
	Make Everyone a Sensor	329
	Create Decision Fast Lanes	330
	Value Expertise from the Top Down	331
	Further Reading	331
Chapter 16	Behavior and Culture: Mastering People-Centric Security	333
	What Does Security Culture Transformation Mean?	334
	Describing Transformation in Terms of Cultural Capabilities Maturity	334
	The Cultural Capabilities Maturity Model: Formalizing Cultural Maturity	335
	Supporting Security Culture Transformation with Security FORCE Projects	338
	The Value of a Security FORCE Project	338
	Managing a Security FORCE Project	338
	The Security FORCE Scorecard	340
	Scoring the FORCE Survey Questions, Revisited	341
	Pooling Your FORCEs	341
	Security FORCE Metrics and the FORCE Scorecard	342
	“Are We a Highly Reliable Security Program?”	343
	CSCF and Security FORCE: Aligning Culture and Behavior in People-Centric Security	347
	Chaining Culture and Behavior Efforts	348
	Using the SCDS and FORCE Independently	349
	General Alignments Between Security FORCE and the CSCF	349
	Taking Advantage of Cultural-Behavioral Alignments	353
	Blending Security Culture Diagnostic and Security FORCE Projects for Improved Cultural Maturity	355
	Further Reading	356
Chapter 17	Leadership, Power, and Influence in People-Centric Security	357
	A Crisis of Leadership	358
	The CISO as a Business Leader	359
	Business Leaders as Security Enablers	360
	Security Power Dynamics	361
	“What if I am not a CISO?”	362

	Leadership in People-Centric Security	364
	You Don't Lead Machines	364
	Influence and Transformation	365
	Adapting the CSCF and Security FORCE Model to Leadership	365
	The CSCF, SCDS, and Cultural Leadership	366
	The Security FORCE Model and Behavioral Leadership	367
	Further Reading	367
Chapter 18	Securing a People-Centric Future	369
	The Security of Things	370
	Social Security	371
	As Many Securities as Things to Secure	371
	Framing People-Centric Security	375
	Security Soft Power	375
	Three Takeaways from the Book	376
	Putting People-Centric Security to Work	377
	Two Models, One Goal	377
	People-Centric Security Strategies	378
	Conclusion	379
	Further Reading	380
	Index	381

This page intentionally left blank

Foreword

After having worked in information security for over 20 years, I have come to a simple conclusion: unless we move beyond technology alone and start addressing the human element, we are in a no-win situation. Technology is where every organization should start when managing its cyber-risk, but technology can only go so far. We have hit that point of diminishing return. We can no longer ignore the human factor in information security. Lance's book is a breath of fresh air. He creates a new chapter in how organizations should manage their risk, not just at the technical level but at a human level. What makes Lance's book so powerful is that he not only backs the book with tremendous research and academic studies, but also brings in real-world application.

I first met Lance through his previous book, *IT Security Metrics*. It was one of the few books I had found that attempted to measure the human side of information security. He went beyond just hard numbers and acknowledged the softer side of our world. Since then, I have been working with Lance and have come to recognize and respect the unique traits he brings to our community. As a PhD in social science, Lance brings academic rigor to our world, but even better, he brings the skills necessary to understand *how* people and cultures work. Combined with more than 25 years of real-world, global experience in the information security field, his philosophy and practice bring immense wealth to the security sector.

What I love most about this book is that anyone can read it. Lance helps you understand what culture is and why it is an issue for information security, ultimately providing a framework to manage and measure it. I hope you are as excited as I am about this opportunity to both better understand a challenge we all face and leave this book better armed to do something about it.

–Lance Spitzner
Research & Community Director, SANS Securing The Human

Acknowledgments

A lot of people had a hand in making this book happen, both directly and indirectly, and I want to try to acknowledge all of them. I owe so much to Meghan, my editor at McGraw-Hill Education, who took a chance on an idea that she believed in and fought for. There would be no book without her. I also want to thank David, my friend and mentor for so many years. I like to tell my son that he'll have lived a fortunate life if he has a friend as good as David has been to me.

I am indebted to the entire team at McGraw-Hill Education, especially those who supported getting this book out the door. Amy, Janet, Brandi, Jared, Bill, and Anubhooti, you made this experience rewarding and challenging, and I can't tell you how thankful I am for your help and your insights. Thanks as well to the many people behind the scenes at McGraw-Hill Education who I never got to know personally, but who contributed their own efforts to this project. Big shout-outs go to Lance Spitzner, for contributions of both words and deeds as I was putting this book together. To Ira, who always gives me his honest opinion on everything, which I value more than I tell him. To Ric, for walkabouts and conversations all over the world. And to Ken, Mike, Pablo, Steve, and Troy, for being true friends in good times and bad. Also my gratitude to Dr. Phil Doty, one of the smartest people I have ever met, who first suggested I read Karl Weick all those years ago.

There is very little truly original knowledge in the world, and scholars and researchers everywhere create new contributions by mining the efforts of others who have gone before them. I am a prime example, and I want to acknowledge the work and contributions of all the academics and practitioners cited, quoted, and adapted in this book. Thank you so much for lending me such excellent shoulders to stand upon as I looked around.

Finally, a dedication is not quite enough. My wife and son deserve the last word. They gave me space and freedom, without complaint, to take on one of the most consuming activities I have ever experienced. And they did it not once, but twice. Thanks, you two.

Introduction

The origins of this book are diverse. It comes from several different ideas I've explored or been interested in over the years, ideas that traced their own individual orbits inside my head and then gradually came together into a concept I felt compelled to write about. I decided I wanted to write a book about security culture not long after I finished my first book, *IT Security Metrics*. I didn't call it "security culture" at the time or think about in those terms. I just knew after I finished the first book that I wasn't actually finished.

A good friend commented to me after reading *IT Security Metrics* that he thought one of my most important points was how valuable qualitative data and measurement can be to information security programs. It made me glad to hear him say that, because it was one of the reasons I had written the book in the first place. I wanted to add something new to a conversation that was already taking place in our industry. Having recently finished a dissertation in the social sciences, one that relied on both quantitative and qualitative research methods, I thought the security metrics literature was overemphasizing quantitative inquiry and analysis and missing out on the value of qualitative approaches. Often, security professionals I encountered criticized qualitative data and downplayed its usefulness, but these same folks many times didn't even use the term "qualitative" correctly or understand how qualitative research actually works.

In *IT Security Metrics*, my advocacy for qualitative approaches was deliberately gentle and conciliatory, toned down in the hopes that I might get some readers interested but not alienate too many of them. I still gave quantitative approaches top billing, which was fine. The book seemed to have the intended effect. Some people wanted to explore qualitative information security metrics more deeply, while those who did not could safely ignore those particular chapters.

In the years since I finished the first book, a lot of things have happened and a lot of things have changed. Perhaps the two most impactful events as far as *People-Centric Security* is concerned were a global financial crisis and a crisis of confidence in the information security industry. The former has passed, although we still feel its lingering aftermath, while we are still smack in the middle of

the latter. In the case of the financial meltdown, a complex global system that had become opaque and automated broke down as a direct result of irrational human behavior. Safeguards that were meant to prevent such collapses didn't work. In the case of information security, a similarly complex global system that is also highly dependent upon technology solutions seems to be breaking down. The collapse is not as spectacular or compressed as the financial crisis was, but it still feels pretty catastrophic when every week seems to bring news reports of millions of people's data being stolen, public accusations of spying and sabotage against governments and criminal organizations alike, and trade conferences where the industry that makes security products will be the first to tell you it has failed and that literally everyone has already been successfully "owned" by the bad guys.

I found at the center of all these things interesting questions of complexity, of the limits of technology solutions, and of the power of human behavior for good and for bad. Society is becoming more technical and more social, each driving and extending the other. Social networking, sharing economies, and the Internet of Things (or Everything) promise to make our world more interconnected and more complex than ever in human history. They also promise to make the idea of people and machines being separate more meaningless than ever before. We're not exactly at the point where everyone becomes a cyborg, but in a world of wearable technology, amazing prosthetics controlled by the user's mind, and body implants with embedded computing and Wi-Fi capabilities, the idea isn't exactly hyperbole.

What happens when you can no longer tell the human infrastructure from the technology infrastructure? That's a question that has as many philosophical implications as practical ones. I'm not trying to address the philosophical points in this book. But I am going to draw a bit of a line in the sand on the practical side of the question, specifically the one that we face in information security. Culture has long been a word associated with how a particular group of people sees the world, including what that group believes and how those beliefs influence the way the group lives. Culture functions at different levels, including geographical, ethnological, and religious levels. Culture also functions at the level of organizations, such as companies and governments, which are perhaps more artificial and less organic than families, tribes, and religions, but which have come to dominate our world just as much. The company I work for has a culture. So does the information security industry. And those cultures, as much as anything else, drive why people do what they do. Our culture has become technological, so we have to understand technology to decipher it. But our technology has also become cultural. If you want to know why a technology system succeeds or fails, whether it be a financial system or an IT system, you have to also understand people.

Which brings me, if in a roundabout way, to this book. InfoSec has always preached the triad of “people, process, and technology” as essential for good, effective security. My experience in the industry has been that technology always comes first, followed by process when we can manage it, and people when we get around to them. The main role people play in information security tends to be that of a problem waiting to happen, an insider threat, a negligent user, or just an annoyance to be automated out of existence as best we can. This book is my attempt to invert that, to put people in the center of information security programs and practices. Sometimes people will be threats, but more often they will be the untapped resources with the solutions to many of security’s current challenges. Thankfully, I’m not alone in believing that people-centric security is the future. The security industry is beginning to realize that technology can only take us so far. As InfoSec programs hit the point of diminishing returns on their technology investments, they must look for other reserves of effectiveness and value. I hope this book helps, in some way, to facilitate the realization of that value.

Who Should Read This Book?

I wrote this book for everyone who has ever wondered why, despite our best efforts and most sophisticated technology solutions, information security seems to be failing more now than ever. InfoSec has become so big and so dispersed across different specializations and disciplines that there’s not really even a single field anymore. We have information security, IT security, information assurance, cybersecurity, and others all maybe referring to the same thing, but maybe not. As an example, throughout this book I’ll refer to our field as information security, or InfoSec for short, which is indicative of my own professional history, preferences, and experience. At the leadership level, however, no matter what you call it, chief information security officers (CISOs) have to run their programs as a business, in partnership with other, non-security executives. At other levels, practitioners will have their own preferences and opinions of what constitutes our field. Everyone has their own concerns about the best way to protect the information assets that are crucial to enterprise success. That being said, there are several groups I can mention who might find value in ideas about how to measure and change security culture.

CISOs

I use “CISOs” as a catch-all to include any organization’s InfoSec leadership, regardless of official title. If you’re in charge of managing security for your company,

you are the chief no matter what your job title is. As leaders, CISOs are the people best positioned to actually manage and change an organization's culture, including its information security culture. But you can't manage what you can't measure, so having a way to analyze and articulate security culture becomes central to impacting and improving it. The techniques and methods I lay out in this book can give CISOs that analytical capability, enabling them to add InfoSec culture to their strategic objectives and roadmaps.

Non-security Organizational Leadership

For every senior executive or board member who has struggled to understand what a CISO is talking about or to make sense of the fear, uncertainty, and doubt over security breaches bombarding them in the media, I hope this book helps to break down how security professionals think. If you can understand what motivates a person, you can find a way to work with them, to compromise for mutual benefit, and to resolve conflicts before they become dangerous. This book talks a lot about the competition between values and cultures within an organization, including values and cultures outside of the InfoSec program. My sincere hope is that non-security leaders and managers can use this book as a way to better understand information security, and where the security team is coming from in terms of values and priorities. Even better, maybe these same non-security professionals will be better able to explain to security practitioners where everyone else in the organization may be coming from, especially when those values and priorities clash. InfoSec programs are often seen as impeding rather than enabling the business, which leads to tension and conflict between stakeholders. This is, at heart, a cultural challenge, one I hope this book can help people to overcome.

Training and Awareness Teams

In the book, I refer to security training and awareness teams as the “tip of the spear” for cultural transformation in the industry today. I have a great deal of respect for anyone who takes on the challenge of educating and mentoring others, and when the subject is protecting and preserving an organization's information and technology assets, that challenge can be even greater, the stakes higher. This book is not a training and awareness book, but the methods and tools provided in the book can absolutely help security awareness programs. One major contributor to security incidents and data breaches today is that we don't include enough human and organizational behaviors in our repertoires of risk. The frameworks I offer here can help expand that knowledge base and give training teams more options and more areas of focus with which to be successful.

Security Operations

Again, I talk about “security operations” generally, as a blanket reference to all the people responsible for keeping the InfoSec program running. Whether you are an analyst, an incident response manager, a developer, or some other information security specialist, you are part of what creates and transmits your organization’s security culture. That means you have power, even if it doesn’t always feel that way.

This book can help give information security professionals a language with which to express what they do and why, and to communicate with others who may not understand or agree with them. I don’t expect people to read this book out of some appeal to the cliché that “everyone is responsible for information security,” although that’s true. Instead, I would encourage you to read the book for the most self-serving of reasons, namely to be able to justify why you do things a certain way and to explain to others why they should give their support (financial, political, time) to help you get them done. The most common question I get asked by customers is if I can help them justify information security measures, activities, and budgets to upper management. In my experience, senior business leaders speak the language of culture and organizational behavior more fluently than they speak the language of technology and security. This book can help translate the cryptic dialect of InfoSec into speech that business stakeholders understand.

I have drawn on years of consulting experiences in developing the case studies and stories in this book. Names, details, and circumstances have been altered to protect the identities of specific organizations.

Companion Website

Accompanying this book are templates that you can use in your own organization to transform your information security culture. To call your attention to these templates, the Download icon has been included where these templates are referenced throughout the book. These templates, as well as other resources on organizational and InfoSec culture, are available to you for download from <http://lancehayden.net/culture>. The templates are fully customizable so that you can use them to their best effect within your organization.

A small icon consisting of a black rectangle with the word "DOWNLOAD" in white, all-caps text, positioned above a black downward-pointing arrow.

A note on URLs. Throughout the book, I use only top-level URLs, even when pointing readers to specific documents or web pages. This is deliberate. In this age of e-books, a broken link can be troublesome, sometimes even resulting in a book being made unavailable through some vendors. To avoid this problem, I have avoided links that are more likely to change or die. In all cases, it should be a simple matter to search the site I give in the link, or the Internet more generally, for titles and authors. I apologize for any inconvenience this may cause.

This page intentionally left blank

PART



Understanding Your Security Culture

This page intentionally left blank

CHAPTER

1

Information Security: Adventures in Culture Hacking

You don't have to go digging through technology news feeds for evidence that the world of information security is in a state of crisis. Data breaches are all over the mainstream media. Enormous in scale and frightening in their implications, major security incidents seem to be happening with alarming regularity. When it is not shady criminal hackers perpetrating the theft, we worry that it might be a hostile government gearing up for a new kind of warfare, or even our own government embracing a new age of Orwellian surveillance possibilities. And the message that resonates from the pages of information security industry magazines and websites to the keynote speeches of industry conferences and the marketing brochures of product and services vendors is, *InfoSec is broken somehow—it doesn't seem to work anymore.*

Maybe. Society has undergone profound changes with the widespread adoption of digital, networked information technologies. Some theorists speculate that these changes are structural, representing not just new features of traditional society, but new definitions of society itself. In this view, we are going through changes like those that happened when human beings stopped being nomadic and established agriculture and villages, or like the transformations that took place during the Enlightenment, or as a result of the Industrial Revolution.

Such evolution means that everyone, including the information security industry, better be ready for changes unlike anything we've previously experienced. Technology has become social, centered around people, and information security must become equally people-centric if it hopes to succeed. We not only have to do things better, but we have to invent whole new ways of doing them. That means looking at things that have traditionally made security experts, especially technologists and engineers, uncomfortable. Things that are hard to measure or automate. Things like people, including their beliefs and assumptions as much as their behavior. Things like culture.

Burnt Bacon

I first realized the power of culture in information security a few years ago at a supplier conference hosted by a customer. Dozens of reps from different vendors filled a large hotel ballroom reserved by our host. After we had all grabbed our coffees and sat down, the executive running the event called the meeting to order with a safety briefing. He introduced us to our safety officer, let's call him Bob, who also worked for the customer. Bob was not an executive or even a manager. But before turning over the microphone to Bob, the executive made it clear that, in terms of our physical safety and security, for the next two days Bob might as well be the CEO.

I had not expected the briefing, but I wasn't very surprised. The company running the conference operated in several hazardous industries and prided itself on the "culture of safety" it instilled in employees. Bob spent about five minutes running us through a review of safety protocols for the event, pointing out all the exits, telling us which we should use in the event of an emergency, and even declaring a rallying point across the street. Should something happen that required us to leave the building, everyone was required to meet at the rallying point for a headcount prior to returning or taking whatever other actions Bob deemed appropriate. Once he had finished, Bob took his post at the back of the ballroom and the day's activities commenced.

I *was* surprised when we returned from the first day's lunch break and the executive again handed Bob the mike so that he could repeat the same briefing we had listened to only four hours before. "Wow," I thought. "These people take safety seriously." I had never experienced that kind of briefing before at any of my own company's meetings, much less two in the same day at the same event!

Coincidence is a funny thing. Just over an hour after our post-lunch briefing, the hotel fire alarm began to wail. On reflex, everyone turned around to look at Bob, who immediately slipped out of the room. Within a minute, the alarm stopped. A minute or two later Bob returned with one of the hotel managers in tow, who was obviously trying to explain something. I watched Bob shake his head "no," prompting the manager to leave. Ten minutes later, I was standing with my fellow vendor representatives across the street as Bob took a head count.

We found out later that the manager had contacted Bob to tell him the fire alarm had been triggered by a small grease fire in the kitchen, but that it had been contained and posed no danger to our meeting. Bob had not bought the explanation and had triggered an evacuation anyway. We were the only ones to leave the hotel after the alarm, and we caught more than a few curious glances from people passing by. Once Bob was satisfied everyone was present and that the hotel was not actually on fire, he gave the all clear and we filed back into our seats in the ballroom. Despite the minor nature of the fire and the fact that unnecessarily evacuating had cost us nearly an hour of our packed schedule, the executive never gave a hint of annoyance. Instead, he called us back to order by spending another few minutes praising Bob's decision and reminding us that, for his company, safety came before anything else.

The second morning of the conference consisted of breakout sessions scattered in smaller rooms throughout the hotel conference center, but they began only after our morning safety briefing was complete. We broke again for lunch, and when we returned to the ballroom in the afternoon, the executive was waiting for us. He was not happy. Standing in front of the room, he held up one of the vendor packets

each of us had received at the start. Stamped “Highly Confidential” on every page, the packets were the blueprints of the company’s forward-looking IT strategy, including strategic competitive differentiators enabled by technology adoption.

Waving the packet slowly so that we all could see it, the executive chewed us out, describing how the document he held had been discovered in one of the empty breakout rooms during lunch, left there by someone in the room. He explained with obvious irritation that such blatant disregard for protecting sensitive corporate data was unacceptable, especially in a room that included many information security professionals. If it happened again, he warned us, there would be hell to pay. And with that, we started up again, beginning once again with our mandatory safety briefing.

Safe and Not Secure

An important characteristic of culture is that it tends to be invisible, functioning just below our conscious awareness of its influence. But that often changes when we find our own cultural norms challenged, and suddenly we see patterns and conflicts jumping out at us from the shadows. Take, for example, the stark contrast between my customer’s *safety* culture, where the response to the possibility of an incident brought all business to a stop and triggered emergency action plans, and the customer’s *security* culture, where an actual security incident resulted in nothing more than a stern talking-to. The two completely divergent responses to essentially the same thing, a failure incident, made the differences between the safety and security cultures of my customer stand out from one another like black and white. “Wow,” I thought, “one of these things is not like the other.” It was astounding.

My customer believed they had a strong culture of safety. They also believed they had a strong information security culture. But culture is defined by behaviors, not beliefs. The completely different behaviors they exhibited between the two incidents showed where their priorities really lay. Had the executive treated the failure to secure sensitive information like Bob had treated a burnt rasher of bacon, we would have stopped the proceedings immediately until he resolved the problem. Instead of ordering an evacuation, he would have ordered everyone in the room to hold up their vendor packets. The documents were controlled, and at least one person would not have had one.

What Were You Thinking?

I found myself obsessing over the experience for the rest of the day. It distracted me from focusing on the presentations and the interactive sessions. I was distant

and disengaged. Why had the executive just let that security incident slide so easily? He had been visibly angry over it, but he could have done much more than scold us. Was he worried about embarrassing people? Had the evacuation thrown us so far off schedule that he was just trying to make up for lost time and not delay the event further? Thinking that maybe he intended to follow up later and try to track down the perpetrator some other way, I checked for unique identifiers on my packet that could have tracked it back to me directly. I found nothing of the sort.

For a little while, I got depressed. I had traveled a long way to attend a meeting that was all about how important security was to this company, only to watch a senior executive get upstaged by a junior employee when it came to taking action in the face of risk. The response to the security incident called into question the whole purpose of the conference. If the company wasn't going to take action when faced with a security breach involving one of their own information security vendors, how were they ever going to protect themselves from the real bad guys? It would all be technology products and lip service. They didn't care enough to make a real change. I found myself thinking, "They should put Bob in charge of information security."

Then I realized something else. I considered the real, physical harm that I knew this company had seen as a result of lapses in workplace safety. People had been injured on the job, had even died, in the decades that the firm had been working in the industry. I knew the firm had also experienced information security breaches in the past, but my impression was that these failures had rarely risen above the level of a moderate inconvenience. People had a bad day, to be sure, but at the end of it everyone went home safely. If the information security culture was not as strong as the safety culture, it was because the world of information security just didn't *feel* as dangerous as the world of workplace safety. No matter what they said, this company could not think about data security the same way they thought about physical safety. Those cultures could exist side by side, but the assumptions and beliefs that drive behavior, born of experience and observation, were just not the same. I was fascinated and, once more able to focus on the customer, made a mental promise to research the topic further.

So here we are.

Culture Hacking

This book is about culture. It is about understanding it and about transforming it. You can even say it's about hacking it. And when I say *hacking*, I mean hacking in an old-school sense, the hacking that Steven Levy described in *Hackers: Heroes of the Computer Revolution*. Before the term evolved (some might say devolved) into

today's more familiar usage, with all its implied negativity and criminal inferences, hacking described a process of gaining knowledge about a system by exploring and deconstructing it. This knowledge would then be put to use to make that system better, more innovative and elegant. The MIT hackers that Levy wrote about dealt in computer software, the programs and digital code that define how those systems function. But systems, code, and hacking don't stop there.

Software of the Mind

Researchers and experts in organizational culture talk about their topic in ways that would not be completely unfamiliar to computer engineers. There are many frameworks and metaphors for describing organizational culture, but all converge on the idea that culture is a shared set of norms, values, and routines that serves to define how people behave together in organized group settings. If you have ever started a new job, then you have probably experienced a cultural shift as you had to learn how things were done at your new organization, and maybe some of those things were completely foreign to you. But as you learned the ropes, as the culture was transmitted to you and you became part of it, things that you had to think about became automatic and unconscious behaviors. It's almost like the organization programmed you to function within it.

Geert Hofstede, one of the more influential scholars in the field, talks about organizational culture in just this way. For Hofstede, culture is "software of the mind" that allows individuals to align their thoughts, beliefs, and actions in order to solve specific problems. Nowhere does Hofstede, or any other culture researchers I am familiar with, claim that people are programmable in the same way computers are. But these experts do look at organizations as complex systems that share similarities with computers and networks.

By using metaphors drawn from software and computing, we can conceptualize and identify means of understanding how culture can be observed, measured, and changed. Thinking about organizational culture as a different kind of software, with its own codes and programming techniques, makes the hacking analogy a lot more applicable. In fact, the security industry already uses the analogy all the time when talking about social engineering. The idea of hacking people is not new or even very controversial in our industry. But social engineering has always focused primarily on individuals, treating each potential victim as an independent system that must be exploited. You can automate social engineering, as does an attacker who conducts mass phishing attempts by using automated group e-mail tools, but this only allows the attacker to target individuals more quickly and efficiently. It's simply a question of scale.

Hacking culture is different from hacking computers. It means understanding and exploring the relationships between people, the drives and motivations that cause many unique individuals to behave in very similar ways, as a group. Instead of trying to affect the behavior of individual people making specific decisions, a culture hacker is more interested in understanding and changing the entire group's behavior, by changing what that group thinks and believes. Part of hacking is about elegance and efficiency, the ability to produce the greatest effect with the least effort. If you focus on my individual behaviors, trying to change them one at a time, you will be lost in an infinity of inputs and outputs. But if you are able to understand and change my beliefs and assumptions, you will have tapped into the programming that drives all my decisions.

Hacking a person's belief systems may seem kind of creepy, and culture hacking can certainly be put to evil uses. But hacking has never just been about breaking into computer systems illegally or immorally for illicit gain. That's a narrow definition that has, unfortunately, come to be the most associated meaning of the word, thanks to the media and, ironically enough, the security industry. But hacking is much more than that, with a longer history than the one information security has tried to impose on it. Culture hacking is similar. I didn't invent the concept, and it's been around for a long time. I just believe it's a very useful way to think about the challenge of people-centric security.

A Brief History of Culture Hacking

The first people to call themselves culture hackers came from the worlds of activism, fashion, and art. They wanted to shape the way the world looked at itself, to shake up the status quo, and to pull the curtains back on people's preconceived notions. For Mike Myatt, a leadership expert and author, hacking in organizations involves breaking down existing codes and complexity, finding alternatives, and replacing out-of-date or inefficient processes. That's old-school hacking.

Culture hacking is pre-digital, going back to practices like billboard jamming, literally changing the messages on real-world roadside billboards from advertisements to more ironic or anti-corporate messages. These techniques date back to the 1970s, developing in parallel with phone phreaking and the beginning of computer hacking. It wasn't about stealing or defacing private property; it was about retaking control of the system from those who had corrupted it, to make it free again. This was the '70s, remember.

Though it started out fueled by flower power, culture hacking has proven remarkably resilient. As the world changed, so did the focus of the movement. Culture hacking and technology merged with the creation of groups like the