# THE SECURITY CULTURE PLAYBOOK

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

PERRY CARPENTER
KAI ROER

WILEY

# Table of Contents

## List of Tables

Chapter 12

## List of Illustrations

Chapter 1

Chapter 2

Chapter 3

Chapter 6

Chapter 8

Chapter 9

Chapter 10

Chapter 12

Chapter 13

# 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 *21$^{st}$ 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

# Introduction

> We're here to put a dent in the universe. Otherwise, why else even be here?
>
> *Steve Jobs*

**S**o, you're interested in security culture. You are not alone. The use of the phrase “security culture” has been steadily increasing over the past few years as organizations seek to combat the ever-present, daily drip of data breaches.

Somehow, despite all the great advancements in security-related technologies, we are faced with a simple truth: Technology, alone, is not enough. It does not offer sufficient protection against breach. Cybercriminals inevitably find ways to bypass the technology by targeting vulnerable humans; or a malicious or negligent insider may know just the right “work around” to effectively nullify your defenses. That's a recipe for a bad day.

Security leaders and business executives are coming to recognize that it's time to pay close attention to a long-neglected layer within their security stack: the human layer. But, you may ask, doesn't that mean that we should be talking about security awareness? The answer is both yes and no. Awareness is definitely part of the answer, but, by definition, simple awareness can take you only so far. Heck, even the old G.I. Joe public service announcements got that right. If you remember, they ended with the tag line, “Now you know. And knowing is half the battle.”

For far too long, organizations have fallen into the trap of equating security awareness (information sharing) efforts with behavior change.

> *For far too long, organizations have fallen into the trap of equating security awareness (information sharing) efforts with behavior change.*

We all know, however, that knowledge doesn't always change behavior. Tons of people will tell you that they know they should adopt better behavior patterns around what they eat, their financial habits, and more. So, in the same way that technology alone is not sufficient for protection, knowledge alone isn't the answer either.

To add an effective human layer of defense, we need to embrace what is commonly referred to as the ABCs of cybersecurity: awareness, behavior, and culture. That recognition is why we are seeing a surge in people using the phrase “security culture.” But here's the thing: So many people are throwing around the phrase without actually knowing what it means. They know that a good security culture must be a positive thing, but there is no precision or general agreement about what a good security culture looks like or how to achieve this promised security culture goodness.

That creates a dilemma. Security culture becomes this thing that has a lot in common with Bigfoot, the Abominable Snowman, or the Loch Ness Monster. People swear that it exists, but they have a hard time producing anything other than the equivalent of fuzzy photos and rambling stories of how they once saw one. And that's why we wrote this book.

> *Security culture becomes this thing that has a lot in common with Bigfoot, the Abominable Snowman, or the Loch Ness Monster. People swear that it exists, but they have a hard time producing anything other than the equivalent of fuzzy photos and rambling stories of how they once saw one. And that's why we wrote this book.*

We're here to make security culture something that is not only understandable, but also measurable and manageable so you can finally get a handle on how to effectively engage your human layer of security and reduce human risk in your organization.

So let's go on a journey together—a journey to unlock the mysteries of security culture. Your guides (the collective “we” that you've been seeing throughout this short introduction) are Perry Carpenter and Kai Roer. Between the two of us, we have over 35 years of experience studying and consulting on various aspects of security culture. Seriously, we won't bore you with our bios and CVs here. You can find those elsewhere in this book. Just know that you are in good (virtual) hands as we guide you through this journey.

The path awaits. Let's begin.

Perry Carpenter & Kai Roer

February, 2022

## What Lies Ahead?

Our goal in writing this book is to add much-needed precision and guidance to the security culture conversation. We believe the security industry is at a tipping point where leaders are ready to accept that technology is not a panacea. There have been so many great advances in security-related technologies over the past few decades, but those advances are not stemming the tide of breaches. Yes, those advances made technology-dependent hacking much more difficult, but they created the unintended consequence that our people are now the primary target. As an industry, we've been so focused on (and enamored with) technology that we've ignored the human side of the equation.

As leaders now seek to build their human-layer defenses, it is important that they move quickly and effectively. We can't afford to get this wrong. As such, our focus over the next several chapters will be to add much needed clarity about security culture: what it is; what it comprises; how to measure its subcomponents; and how to shape those all-important security-related facets of your organizational culture.

Here's a quick breakdown of what's to come.

## *Part I: Foundation*

Part I is all about building a foundational understanding of why security culture is a critical, *got-to-pay-attention-to-it-now* topic. We discuss the current issues with defining “security culture,” offer some hints to an ultimate definition (yeah, you'll have to wait a bit before we spill the beans on that one), and why security culture is a board-level imperative. We'll also provide some tie-ins with Perry's earlier work, *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors*.

## Part II: Exploration

Part II is all about exploration. We focus on giving concrete examples of what a strong security culture looks like and what the consequences of a poor security culture can be. We'll put organizational culture and security culture under a microscope and examine the various subcomponents we find. Along the way, we will throw in some concepts from sociology, organizational culture management, and a few other disciplines. You'll also gain valuable insights from culture experts outside of the cybersecurity domain.

### *Part 3: Transformation*

Here is where the proverbial rubber meets the proverbial road. Part III is about doing the work. It's about transformation. We'll walk you through the Security Culture Framework, a process that Kai developed over 15 years ago for getting a handle on security culture so that it can be improved. Since its creation, this process has been adopted by organizations and governments around the world. And, because anything worth managing is worth measuring, we'll take a deep dive into how to scientifically measure security culture across seven dimensions, and we'll give an overview of the Security Culture Survey, a tool that Kai and his team created over a decade ago. Since that time, it's been honed into a finely tuned scientific instrument that's been used to collect and analyze the largest security-culture-related dataset on earth. We'll also discuss culture-related gotchas, sticking points, and more. In the last bit of Part III, you'll hear from a number of security experts as they discuss security culture, and we'll leave you with some valuable tools and insights that so you can immediately leverage everything from this book. You'll be able to discuss security culture with confidence, measure maturity, gain executive support, and more.

## Reader Support for This Book

We've also created a resource site for this book where we'll upload new worksheets, research studies, and other useful security culture-related information. It's at SecurityCultureBook.com.

## *How to Contact the Publisher*

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line “Possible Book Errata Submission”.

## *How to Contact the Authors*

We appreciate your input and questions about this book! Connect with Perry or Kai on LinkedIn at www.linkedin.com/in/perrycarpenter and www.linkedin.com/in/kairoer.

# Part I
# Foundation

Welcome to the journey! In Part I, we introduce the concept of security culture, why it is important, and (most importantly), the fact that you can measure and improve your culture. There's a lot to cover, so let's get started. But even before you turn to the first page of Chapter 1, we think it's important to give you a definition of security culture.

> ***Security Culture:*** The ideas, customs, and social behaviors of a group that influence its security.

# Chapter 1
# You Are *Here*

> The greatest danger in times of turbulence is not the turbulence—it is to act with yesterday's logic.
>
> *Peter Drucker*

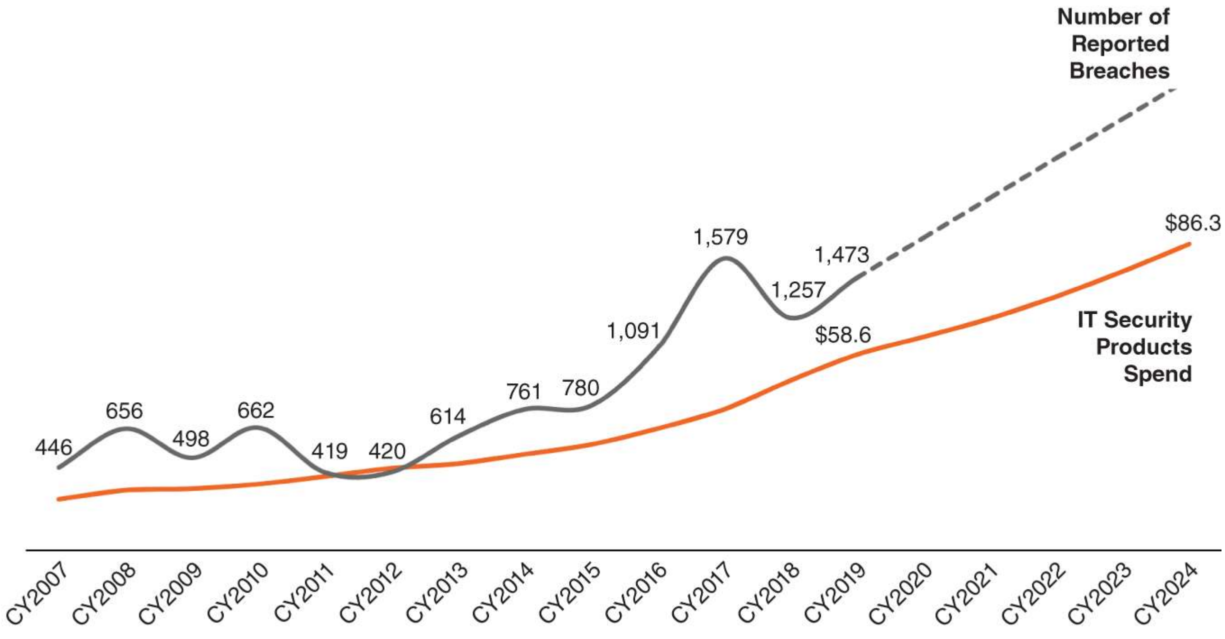
“Security culture” has become a hot topic of late. If you are a cybersecurity or business leader, you've no doubt seen the term appear in online articles, security presentations, and even a few vendor pitches. It's become a buzzword (or buzz *phrase*, if you want to be picky) du jour. Unfortunately, most of the time it is little more than a phrase uttered with gravitas, but devoid of real meaning.

*Security culture* is often confused with security awareness, the implementation of security processes, or even the use of security tools by end users. That initial misidentification becomes even more confusing because each of those things can feed into, or become an artifact of, security culture—but they are not in and of themselves security culture. Security culture is something different, something unique that is undeserving of the confusion that all too often surrounds it. And you know that; otherwise, you wouldn't be reading this book.

Our purpose here is to add precision and clarity to the topic. And, although we could easily fill several hundred pages with great content about security culture, that's not what this book is about. This book, dear reader, is a no-nonsense, (hopefully) no fluff, and (definitely) no BS guide to what security culture is, how to measure it, and how to shape and strengthen it within your organization.

## Why All the Buzz?

For decades, security programs focused on diligently deploying technology-based defenses aimed at keeping cybercriminals at bay. The industry focused on firewalls, intrusion detection and prevention systems (IDSs/IPSs), endpoint protection platforms (EPPs), secure email gateways (SEGs), and more. In truth, the technology has gotten very good. Despite all the focus and spend on security tools, however, the data breach problem is not going away. In fact, it's accelerating faster than the industry can effectively manage via traditional approaches. Figure 1.1 analyzes the amount of money spent on security products since 2007 versus the number of data breaches that occurred each year. The conclusion is clear: The current industry approach is not working.



Source: IDC, Identity Theft Resource Center

**Figure 1.1** Organizations globally have invested massively on cybersecurity, yet breaches continue to increase.

And here's where the buzz about security culture comes in. Leaders are realizing two things:

- Technology-based defenses have gotten so good that attackers are being pushed to hack humans rather than spending weeks, months, or years researching and developing effective attacks to defeat technology-based defenses.
- Humans are now the primary attack vector. As such, it's imperative to strengthen the human layer of security.

These two realizations (illustrated in Figure 1.2) have led to a growing interest in human layer defense. This isn't to replace any of the technology-based layers—those are still needed. But this is to strengthen a much-needed additional defensive layer.

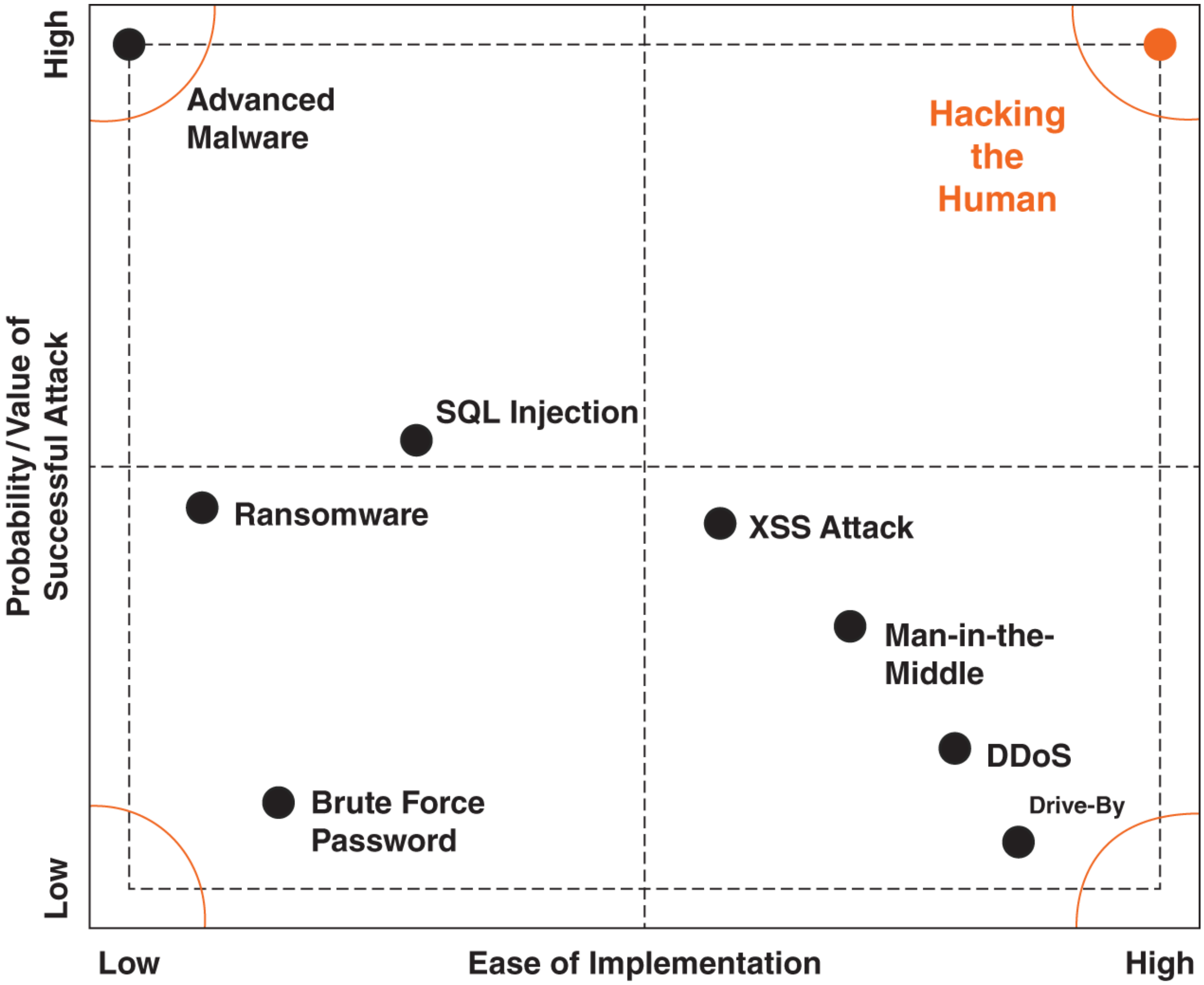


**Figure 1.2** Hacking the human yields the highest ROI for attackers.

## The Technology-Based Defense vs. Human-Based Defense Debate: A False Dilemma

You've undoubtedly been presented with this dilemma before. Someone says that it's worthless to focus on the human side of security because, no matter what, there will always be someone who will fall for a phishing email or make some other error. In short, their argument is that the human defense isn't 100 percent effective, so it can't be relied on and doesn't deserve an investment of time, energy, or funding.

You'll even hear some make claims to the effect of, “only technology will help an organization prevent security issues.” This type of thinking has been prevalent in security circles for decades and has led to the situation that we're in right now, where the human layer has been neglected.

A quote from the preface of Bruce Schneier's book *Secrets and Lies* is fitting here. Bruce ends the preface with these words, “[a] few years ago I heard a quotation, and I am going to modify it here: If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology” (Schneier, 2000).

The following is an excerpt from Perry's book, *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors* (Carpenter, 2019). The excerpt does a good job summarizing why this is a false dichotomy. This shouldn't be presented as an either/or dilemma.