INSIGHTS FROM A CYBERSECURITY CAREER

LESSONS FROM THE FRONTLINES

ASSAF KEREN

WILEY

Lessons from the Frontlines

Insights from a Cybersecurity Career

Assaf Keren

WILEY

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

Library of Congress Cataloging-in-Publication Data has been applied for:

Paperback ISBN: 9781394395385
ePDF ISBN: 9781394395422
epub ISBN: 9781394395415
oBook ISBN: 9781394395439

Cover Design: Wiley
Cover Image: © Vecteezy.com

To every security professional who has ever felt overwhelmed by the responsibility, isolated by the challenges, or uncertain about their leadership journey: this book is for you. The work you do matters, and you don't have to figure it out alone.

And for my dad, may he rest in peace.

Contents

Acknowledgments

To Lilach, Noa, Maya, and Niv who supported me through the long hours, missed dinners, and late-night incident responses that come with security leadership. Your patience during my burnout periods and encouragement during my growth journey continues to sustain me.

To Sri, Dan, Micha, Michael, Aaron, Brad, John, Boaz, and many more of the leaders who influenced my career and taught me what good leadership looks like.

To Pinhas, Dimitry, Renana, Bill, Michelle, Kate, Wes, Anton, Cherie, Ido, Erich, Dan, Ryan, Stan, Ron, Maria, Sri, Adam, and many more people in and out of my teams for your support, friendship, and ongoing education on what good looks like.

And to Jim, Annie, Tracy, Jonas, and the rest of the publishing team who helped make this book a reality.

About the Author

Assaf Keren is the Chief Security Officer at Qualtrics, where he leads the company's global security strategy and operations. With over 25 years of experience in cybersecurity, Assaf has a proven track record of driving transformative security initiatives. Prior to Qualtrics, he held senior leadership roles at PayPal, where he spearheaded major security transformations. He is also a seasoned entrepreneur, having founded and successfully sold two cybersecurity companies.

Assaf's expertise extends beyond the corporate world; he has served in military roles focused on defense and security. He holds multiple patents in security technology and has been recognized as one of the industry's most influential CISOs.

In addition to his executive responsibilities, Assaf serves on several corporate boards and advisory panels, providing strategic guidance to both startups and established companies. He is a frequent speaker at major security conferences worldwide, sharing insights on emerging threats and security innovation.

Introduction

If you picked up this book thinking that security leadership is primarily a technical role, I'm going to challenge that assumption from the very first page.

Yes, you need to understand technology, threats, and controls. But after 25 years in cybersecurity—from military intelligence to Fortune 500 CISO roles—I can tell you that the leaders who thrive aren't necessarily the most technically brilliant. They're the ones who've learned to navigate the complex human side of security work.

They know how to build curiosity-driven teams that adapt to constant change. They've developed the grit to recover from inevitable failures and the optimism to inspire others during crisis. They execute without waiting for permission, embrace change as opportunity, and speak the language of other business leaders. Most importantly, they understand that security work is fundamentally about people—protecting them, enabling them, and working through them to create more secure organizations.

This book isn't a collection of theoretical frameworks or generic leadership advice. It's built from real experiences, honest failures, and hard-won lessons from the frontlines of cybersecurity leadership. Every story I share, every mistake I admit

to, every framework I present has been tested in the reality of high-pressure security environments.

Why These Lessons Matter Now

Whether you're already in a security leadership role or aspiring to one, you're operating in a field that's changing faster than ever. New threats emerge daily. Technologies evolve monthly. Regulations shift constantly. Organizations restructure regularly. The traditional approach of developing deep technical expertise and hoping that translates to leadership effectiveness simply isn't sufficient anymore.

The security leaders who succeed in this environment are those who've learned to balance technical competence with human skills. They can read a room as well as they can read a security report. They know when to state reality and when to inspire hope. They build the kind of relationships and communities that make complex security initiatives actually work.

But here's what no one tells you about security leadership: You're going to fail. A lot. You'll make decisions that don't work out. You'll face challenges that overwhelm you. You'll have moments where you question whether you're cut out for this work at all.

I know because I've been there. I've been the incident commander who froze under pressure and let an adversary escape with data. I've been the new CISO who embarrassed himself in front of executives by cataloging problems without offering solutions. I've burned out from trying to control everything and learned the hard way that sustainable leadership requires trusting others.

The difference between leaders who thrive and those who burn out isn't that the successful ones avoid failure—it's that they learn from failure and use those lessons to become more effective.

What You'll Find in This Book

This book is organized around thirteen core competencies that I've learned are essential for security leadership. These core competencies are structured into four parts to guide your leadership journey clearly and progressively.

Part I: Personal Foundations—Cultivating curiosity, grit, and optimism to sustain you through challenges.

Part II: Core Leadership Competencies—Mastering execution, change management, business acumen, diplomacy, and communication.

Part III: The Human Side of Leadership—Addressing mental health, self-care strategies, and building supportive communities.

Part IV: Strategic Leadership—Leading at scale with lessons from startups to Fortune 500s and applying product thinking in security.

The competencies are presented roughly in the order you'll need to develop them, starting with the foundational traits that sustain you through challenges and progressing to the advanced skills needed for senior leadership roles.

Part I focuses on the personal foundation every security leader needs: **Curiosity** to keep learning and adapting, **Grit** to work through inevitable challenges, and **Optimism** to maintain forward momentum even during difficult periods.

Part II covers the core leadership competencies: **Execution** (moving from permission-seeking to intent-based action), **Change Management** (leveraging constant change as competitive advantage), **Business and Finance Acumen** (understanding that we're measured by business success), **Diplomacy** (building the relationships that make security initiatives actually work), and the

communication framework that transformed how I approach leadership: **State Reality, Inspire Hope**.

Part III addresses the often-overlooked human side of security leadership: **Acknowledging Mental Challenges**, **Self-Help Strategies** for sustainable performance, and **Building a Supportive Community** that makes you more effective and resilient.

Part IV focuses on strategic leadership capabilities: **Leading from the Front** (lessons from startup to Fortune 500 leadership) and **Product Thinking in Security** (building solutions, not just defenses).

Given the pivotal moment we are in with the advent of GenAI and Agentic AI, I've incorporated a **case study on AI adoption** reflecting the lessons and frameworks shared throughout the book.

Each chapter combines personal stories from my career with practical frameworks you can apply immediately. I'll tell you about the wall in basic training that taught me about mental limitations, the harsh feedback that forced me to develop real competence, the startup anxiety of watching the runway shrink while trying to pay ten people's salaries, the complete rebuild of PayPal's global security operations, the burnout that nearly ended my career, and the mentors who saw potential in me that I couldn't see myself.

More importantly, I'll share what I learned from each experience and how those lessons translate to practical leadership skills you can develop and strengthen over time.

A Different Kind of Security Book

This isn't a book about the latest threats or cutting-edge technologies. It's not a technical manual or a compliance guide. If you're looking for frameworks for risk assessment or instructions

for implementing security controls, there are excellent resources available elsewhere.

This book is specifically for people who understand that security leadership is fundamentally a human challenge. It's for current and aspiring security leaders who want to learn from someone else's mistakes rather than making all the same ones themselves.

It's for people who are tired of security being seen as the "department of no" and want to learn how to be genuine business enablers. It's for leaders who are struggling with burnout or isolation and need to understand that these challenges are normal and manageable. It's for anyone who wants to build a security career that spans decades rather than burning out after a few intense years.

Most importantly, it's for people who believe that cybersecurity is too important to be left to chance. The digital infrastructure we protect isn't abstract—it's the foundation that enables everything from healthcare to commerce to communication. The work we do matters, and it deserves leaders who can sustain themselves and their teams for the long haul.

How to Use This Book

While I've organized the chapters in a logical progression, each one stands alone and addresses distinct leadership challenges. You might read it straight through, or you might jump to the chapters that address your most immediate needs.

If you're early in your security career, pay particular attention to the foundational chapters on curiosity, grit, and optimism. These traits will sustain you through the inevitable challenges ahead.

If you're already in leadership roles but struggling with execution or change management, focus on those specific chapters and the frameworks they provide.

If you're dealing with burnout or isolation, the chapters on mental challenges, self-help strategies, and community building might be most valuable.

Throughout the book, I've included reflection questions to help you apply these lessons to your own situation. Take time with these questions. The goal isn't just to read about leadership principles—it's to develop the self-awareness and practical skills that will make you more effective.

The Journey Ahead

Security leadership is a journey, not a destination. Every leader continues learning, growing, and adapting throughout their career. The challenges you face will evolve, but the fundamental principles of effective leadership remain constant.

What I can promise you is this: If you approach security leadership with curiosity about what you don't know, grit to work through difficulties, and optimism about what's possible, you'll be able to handle whatever challenges come your way. If you focus on execution rather than permission-seeking, embrace change as opportunity, and build genuine relationships with the people around you, you'll be able to drive meaningful improvements in your organization's security posture.

Most importantly, if you take care of yourself and build the kind of supportive community that sustains long-term effectiveness, you'll be able to have the kind of career that makes a lasting difference.

The cybersecurity field needs leaders who can think strategically while executing tactically, who can balance technical expertise with business understanding, and who can maintain their humanity while dealing with constant threats and pressure.

It needs people who can build careers that span decades and develop the next generation of security professionals.

I hope this book helps you become one of those leaders.

The journey starts now.

PART

I

Personal Foundations

The security leadership journey begins with three core personal qualities that sustain you through every challenge ahead. Before you can effectively lead others, you must develop the internal foundations that will carry you through decades of evolving threats, organizational changes, and high-pressure decisions.

Curiosity drives continuous learning in a field where yesterday's expertise can become tomorrow's blind spot. It's the engine that powers adaptation when new technologies emerge and threat landscapes shift. Without genuine curiosity about what you don't know, security leaders quickly fall behind the pace of change.

Grit provides the resilience to work through inevitable failures and setbacks. Security work is inherently challenging; you'll face impossible deadlines, limited resources, and problems that often lack clear solutions. The ability to persist through these challenges while learning from failures separates effective leaders from those who burn out.

Optimism maintains forward momentum even during crisis periods. While our field requires constant attention to what could go wrong, sustainable security leadership demands the ability to inspire confidence that challenges can be overcome. The leaders who thrive are those who can acknowledge serious problems while maintaining a genuine belief that solutions exist.

The following three chapters explore how to develop and strengthen these foundational qualities through practical frameworks and real-world experiences, providing actionable strategies you can begin implementing immediately to build the personal resilience and adaptability that effective security leadership requires.

CHAPTER

1

Curiosity

The choice that launched my security career happened in the most unremarkable way possible. I was sitting across the desk from my commanding officer, still recovering from leaving the infantry due to health issues, when he casually mentioned they had an opening for intelligence OR information security NCO training.

"Are you interested?" he asked.

The question hung in the air for maybe three seconds, but in those seconds, my entire future shifted.

I didn't know what intelligence meant in practical terms. I had no clear picture of what information security involved. I couldn't have explained the difference between the two paths he was offering. But something in me responded immediately:

I chose information security.

Looking back, I think I had always been drawn to that kind of work—the analytical thinking, the puzzle-solving, the technical

challenges—but I'd never known it was an option or had a clear path to get there.

It was pure curiosity about something I didn't understand but found intriguing. That moment of curiosity—being willing to step into the unknown—set the trajectory for the next 25 years of my career.

And that willingness to say yes to the unknown has become the thread running through every major career decision I've made since.

This randomness taught me something crucial about opportunities in cybersecurity: they often come disguised as throwaway comments, casual invitations, or side conversations. The person making the offer might not even realize they're potentially changing your life. The key is maintaining enough curiosity about the world around you to recognize these moments when they appear.

Curiosity isn't just a nice-to-have trait in cybersecurity leadership, it's the foundation that enables everything else. In our rapidly evolving field, the ability to continuously learn and adapt separates effective leaders from those who get left behind. This chapter makes the case for curiosity as essential for personal growth, career development, and business success.

The Foundation of Everything

Curiosity in cybersecurity is the engine that drives everything else. In a field where threats evolve daily, technologies shift monthly, and regulations change yearly, the leaders who thrive are those who never stop asking questions.

But curiosity in cybersecurity leadership goes deeper than just staying current with the latest attack vectors or compliance requirements. It's about maintaining a beginner's mind even as you gain expertise. It's about questioning assumptions—including

your own. It's about being genuinely interested in how things work, why they break, and what that tells us about human behavior and system design.

My early technical experiences, even the basic website building I did in high school during the early days of the internet, created this foundation. I wasn't trying to become a security professional—I was just curious about how to make things work on the web. How do you get text to appear in different colors? How do you make images load? How do you create links between pages? These were simple questions, but they got me comfortable with the idea that understanding technology meant breaking it down into components and figuring out how those components interacted.

That curiosity about the mechanics of technology, combined with a growing interest in understanding how systems could be compromised or misused, naturally led me toward security work. I didn't have a master plan. I just followed questions that interested me, and those questions happened to lead toward cybersecurity.

This is something I try to remember when I'm hiring or mentoring people early in their careers. Some of the best security professionals I know didn't start with a clear vision of becoming Chief Information Security Officers (CISOs). They started with curiosity about how things work and why they sometimes don't work the way they're supposed to. That curiosity, more than any specific technical skill, is what sustains a long-term career in this field.

From Military to Information Security

The transition from infantry to information security work wasn't just a career change—it was a complete mindset shift that revealed how curiosity could be systematically developed and applied.

Infantry training is about following orders, executing plans, and maintaining discipline under pressure. There's curiosity involved, but it's focused and constrained. You might wonder about the tactical situation or the reasoning behind a particular maneuver, but the scope of your curiosity is limited by your role and responsibilities.

Information security work requires those same disciplines but adds layers of analysis, questioning, and strategic thinking that I'd never encountered before. Suddenly, curiosity wasn't just welcome—it was essential. You're constantly asking: What are we not seeing? What patterns are we missing? What would an adversary do in this situation? What assumptions are driving our analysis?

But perhaps most importantly, information security work taught me that curiosity needs to be disciplined and systematic. You can't just wonder about things randomly. You need to develop frameworks for asking productive questions, methods for testing hypotheses, and ways to distinguish between useful insights and interesting but irrelevant observations.

This transition taught me something that has served me throughout my cybersecurity career: curiosity without structure can lead you down rabbit holes, but structure without curiosity leads to blind spots. The most effective security leaders I know have learned to balance systematic approaches with genuine openness to unexpected discoveries.

The Danger of "Knowing Enough"

One of the biggest traps I see security professionals fall into is reaching a point where they feel they "know enough." They've mastered the fundamentals, they understand their organization's systems, they can handle the day-to-day challenges. The curiosity

that got them there starts to fade, replaced by confidence in their existing knowledge.

This is dangerous in any field, but it's potentially catastrophic in cybersecurity. The moment you stop being curious is the moment you start falling behind. Adversaries are constantly innovating. Technologies are constantly evolving. Business requirements are constantly changing. If you're not actively curious about these shifts, you're not just standing still—you're falling behind.

I learned this lesson the hard way early in my career at the Israeli eGovernment. Coming from military service, I thought I understood technology and security. I had confidence born from successfully completing challenging training and serving in demanding roles. I felt ready to impress my new colleagues with my knowledge and experience.

It took about a week for them to pull me aside and deliver some blunt feedback: "Kid, you don't know what you're talking about."

The words hit like a punch to the gut. I was offended, hurt, ashamed. I went home that day thinking about quitting. How could they be so dismissive of my experience and capabilities? Didn't they understand what I'd accomplished in the military?

But as the initial sting faded, I realized they were absolutely right. I had confused familiarity with a few security concepts with actual competence in the field. I had mistaken confidence for knowledge. I had stopped being curious about what I didn't know because I was so focused on demonstrating what I did know.

That moment was humbling and painful, but it was also a gift. It forced me to rediscover curiosity about areas where I thought I already had competence. It reminded me that confidence without curiosity is just arrogance in disguise.