THE ART OF CYBER LEADERSHIP

Principles for Success

By Matthew Doan

About Booz Allen Hamilton

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no road maps. They rely on us because they know that – together – we will find the answers and change the world.

We solve the most difficult management and technology problems through a combination of consulting, analytics, digital solutions, engineering, and cyber expertise. With global headquarters in McLean, Virginia, our firm employs approximately 24,600 people globally, and had revenue of $6.17 billion for the 12 months ended March 31, 2018. To learn more, visit https://www.boozallen.com. (NYSE: BAH)

THE ART OF CYBER LEADERSHIP

Principles for Success

By Matthew Doan

CYBEREDGE
PRESS

The Art of Cyber Leadership

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9990354-8-1 (paperback)
ISBN: 978-0-9990354-9-8 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from: Amanda Thornhill Morrison, Gary Barnabo, Kim Ann King, Todd Inskeep

Table of Contents

Preface

"I wish you good fortune in the wars to come."

— Ser Arthur Dayne, Game of Thrones

Welcome to *The Art of Cyber Leadership: Principles for Success*. I've written this book because I wholeheartedly believe in its concepts and the need to share them. Within these pages, you'll find a unique perspective on what companies must do to infuse true cybersecurity into their world. In line with the title, call it a "first principles" look at making progress on this front.

Every day, I see organizations struggling to understand where to start or step next with cybersecurity. Their focus is typically on patching vulnerabilities, pen testing, and ensuring they've implemented a complicated amalgamation of tools from a long checklist. However, this isn't good enough. The leaders of these organizations firmly believe that such activities will secure the business, and therefore accomplish the mission. The problem is, they won't.

This book is likely quite different from any other cybersecurity book you've read. Typically, those books delve into security architectures, technical tradecraft, and nascent approaches such as machine learning, advanced analytics, and software-defined networking. They might even present an "MBA" view on measuring risk and communicating it to the board. But that's not what we're going to cover in this book. I'm interested in something much deeper, much more human.

While most of the world is focused on the science of addressing technical cyber challenges, here, we'll dig in to understand the other side of the coin: the art—specifically, the leadership art—required to make cybersecurity a vibrant part of the strategy, operations, and culture of a business.

We'll feature a well-rounded, field-tested set of perspectives on how to lead real change, pulling insights from leading thinkers in the fields of organizational psychology, neuroscience, and military leadership, among others. My hope is that this broad insight will provide much-needed direction for improving and scaling particular skills that are seemingly almost impossible to find—and impossibly valuable—today in the field of cybersecurity.

There are two important audiences for this book:

1) **Cyber leaders**, who must understand and learn which skills to acquire and how to employ them. Chances are, you've arrived at your position through excellent technical aptitude and competent organizational and managerial skills—but without much careful thought about (and skill acquisition on) what it takes to be a game-changing leader.

2) **Business executives,** who need to understand that because the art of cybersecurity is so different from the science, they must look for a completely new set of aptitudes and skills when hiring and cultivating their cyber leaders.

For each audience, we'll supply valuable takeaways about how to inspire and motivate teams, rally them around the cause of cybersecurity, and encourage them to work together against unrelenting adversaries.

It's my hope that this book will accompany you on a long and successful journey as you unlock new potential within yourself, invigorate your teams, test new skills, and fight the good fight.

Matthew Doan

Cyber Strategist, Booz Allen Hamilton

Cybersecurity Policy Fellow, New America

Introduction

"An artist is someone who uses bravery, insight, creativity, and boldness to challenge the status quo. And an artist takes it personally."

– Seth Godin

Everyone knows about the increasing volume and sophistication of cyber threats against an ever-expanding digital attack surface. And whether your scope is to protect corporate networks, the manufacturing environment, the cloud, or revenue-producing products and services, security is an ongoing process, not a product. But there's something missing from this process, and that's people. Not just any people. Leaders. And not just any leaders. We need **great** leaders if we are to win in cybersecurity.

What's required is a rebalancing between the science of cyber technology and the **art of leadership**. We have the tools to build an effective defense. But without qualified leaders, they don't make enough of a difference. And so, the adversaries persist, companies are breached, data is stolen, production operations are impacted, and business availability suffers along with reputation, customer trust, and financials.

In this book, we'll dissect how to enable the science of cybersecurity through the art of leadership: how to become a leader who cultivates passion in others, enlightens and rallies a broad stakeholder community, and coordinates resources and activities that bring real security to an environment.

The bottom line is that **leaders**—not technologies—are the **core enablers** of cyber success. In fact, effectively implemented technology is simply a downstream byproduct of great, artful leadership.

Chapters at a Glance

Chapter 1, "A Baseline of Today," discusses where we are now and how we got here.

Chapter 2, "Principles: A Preview," reviews the four key principles that serve as the foundation for successful cyber leadership.

Chapter 3, "Principle 0: Self-Reflect," weighs in on the importance of level-setting with yourself, being humble, and what it means to serve as a leader.

Chapter 4, "Principle 1: Catalyze," looks at how to cultivate a vision and a long-lasting following.

Chapter 5, "Principle 2: Shape," reveals how to influence your broad stakeholder community and improve your overall odds of success.

Chapter 6, "Principle 3: Orchestrate," discusses how to structure and choreograph resources to serve the business as agilely and optimally as possible.

Chapter 7, "Bringing the Concept to Life," provides additional advice on how to implement the four principles and embody the qualities of a successful cyber leader.

Helpful Icons

TIP

Tips provide practical advice that you can apply in your own organization.

DON'T FORGET

When you see this icon, take note, as the related content contains key information that you won't want to forget.

CAUTION

Proceed with caution, because if you don't, it may prove costly to you and your organization.

Chapter 1

A Baseline of Today

In this chapter

- See how the cyber landscape has evolved
- Learn why security efforts continue to lag
- Understand the need for better leadership, not more tools

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted; none of these measures address the weakest link in the security chain."

– Kevin Mitnick

A Long Time Ago in a Galaxy Far, Far Away

Think back just a decade ago and how vastly different our cybersecurity concerns were. Most threats were data breach related: criminals were thrilled to steal sensitive information or siphon some money, and get out as quickly as they got in. Or nation states sought economic advantage through espionage: exfiltrating some "leapfrog"-worthy intellectual property. Yesterday, we worried about cyber attackers who **stole**. We responded by building ever more elaborate security architectures—but the attacks kept coming, growing in both frequency and sophistication.

Today's cyberattacks have evolved far beyond data breaches (although they have also become more varied and sophisticated). We now worry about threats that **disrupt and destroy**. Essentially, the impact type has changed—moving beyond the theft of information and money to the disabling or wholesale wiping out of critical systems that enable a company to conduct business. And with attacks on certain systems that control kinetic processes, we're looking at health, safety, and environmental issues.

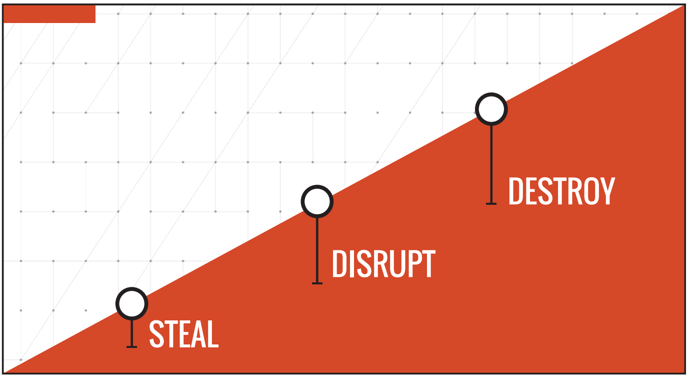


Figure 1-1: Cybersecurity incidents are becoming more frequent and more severe.

Today, with the rise of IoT and the increasing digitization of every business process, we've massively expanded the attack surface. It's mind-boggling. The entire value chain—the supply network, research and development, operational technology (OT)[1], and customer-facing connected products/services—is now open season for attackers.

It's clear we've moved well beyond a time when the accountability for ensuring cybersecurity rested solely with a back-office IT department. There's no way IT can handle it alone. Cybersecurity has become a board-level, business-wide issue—and a potentially existential one at that. Unfortunately, our mindset for approaching this problem is often radically misaligned with what it truly takes to get it right.

[1] As Gartner defines it, OT refers to "hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise" (e.g., manufacturing plants).

You Call That Progress?

While our ability to architect more-secure systems and networks has generated incremental improvements, adversaries have made **massive** leaps forward, basically wiping out those gains. The expanding attack surface helps adversaries by providing increased access to target-rich environments (i.e., a business' crown jewels).

Nation states are installing tools to enable their offense, while criminal enterprises gear up to make millions of dollars from ransomware. The cyber threat landscape has become organized, efficient, and relentless. Organizations not keeping up now have a huge gap in security that has only grown as the years go by, at a time when we should be meeting the challenge head-on and closing the gap. Why is that?

Are business leaders not "in the know"? Surely, we all understand what is happening—cybersecurity is front-page news. This issue is clearly in the face of board members and business executives across all industries. In fact, "upgrading IT and data security to avoid cyber attacks" is the second-most important concern for CEOs (up from 8th place in 2014), according to CSO Magazine's 2017 U.S. State of Cybercrime Survey. So you'd think that, armed with such knowledge, tone-at-the-top action would unlock funding, authority, and ultimately, success. But sadly, that's only happening on rare occasions.

Have we not established a full view of what "good" security looks like? There's a wealth of frameworks to structure a program against and an endless number of security technologies to select and implement. In fact, many companies get stuck in a never-ending loop of planning, testing, and implementing new security tools to counter every new threat vector out there.

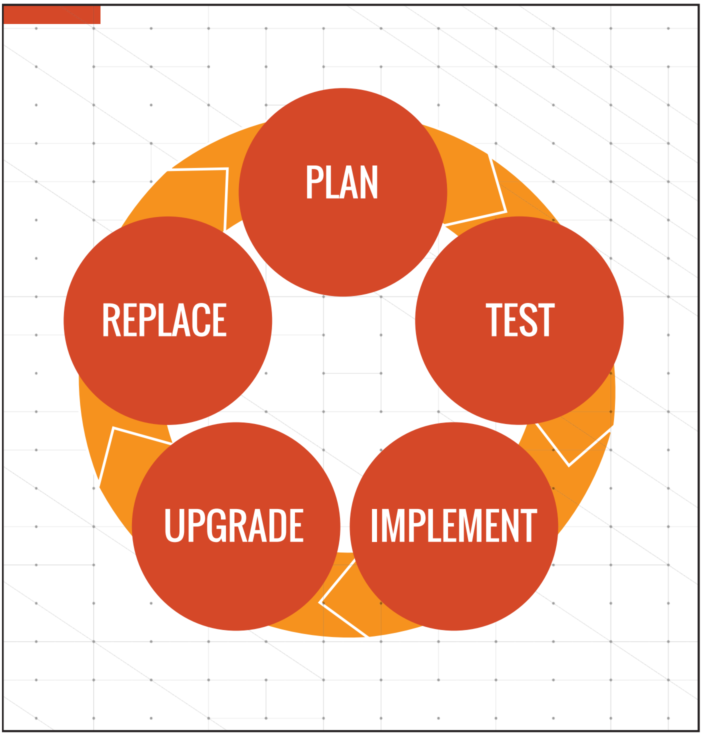


Figure 1-2: Never-ending security tool loop.

Unfortunately, after decades of explosive growth in the cybersecurity market, there are simply too many niche products that don't offer enough actual security. For example, many tools struggle to handle increasing volumes of data and the speed at which it traverses the network.

Companies respond by layering on more and more tools, which lead to excess complexity and cost with little incremental security or return on investment. As companies realize the limits of this approach, they are now looking for a much more holistic and sensible approach to cybersecurity—one that prioritizes people and processes over tools.

The Real Problem Is Leadership

As with any major initiative or function within a business, the weakest link is people. But I'm not talking about uneducated end users who click every link in sight, which is too often the focus of the "people" problem. Instead, we desperately need strong cyber leaders—people who can work within the broader organization and nurture an environment so that the business can thrive. What's lacking today within most security programs is outstanding cyber leadership. I believe we've either ignored or downplayed its significance for far too long.

TIP

Being successful as a cyber leader requires a far different mindset, skillset, and approach than in years past. Gone are the days of the technical guru rising to the top and prospering. While we still need technology superstars on the security team, we also require a whole new breed of people in the leadership position. We need leaders with emotional intelligence and empathy who can motivate their teams and inspire them to go above and beyond—instead of simply leaning on defensive tools, tactics, and architectures. While getting the technical job done is critically important, the cyber leader must also focus on corralling hearts and minds across the enterprise and cultivating a community that embraces cybersecurity. The leader is the great enabler of success.

In the next chapter, we'll introduce four key principles and 16 supporting sub-principles that are fundamental to this new brand of cyber leadership.

Chapter 2

Principles: A Preview

In this chapter

- Learn four principles and 16 sub-principles critical for successful cyber leadership
- Understand the importance of self-reflection
- Learn how to catalyze teams into action
- Discover how to shape your environment to your advantage
- Orchestrate resources with agility as a primary feature

"While values drive behaviors, principles govern consequences."

– Stephen Covey

Before we dive into the four principles and 16 sub-principles that comprise the following chapters of this book, let's review them all together.

These ideas will give you a solid foundation for becoming an inspirational and effective cyber leader.

The Power of Self-Reflection

We start with "Principle 0: Self-Reflect," which weighs in on the importance of starting with yourself before creating change in the world. Being humble, serving others, and pursuing life-long learning and feedback all help you grow. You'll see this principle, along with the others, in Figure 2-1 below.

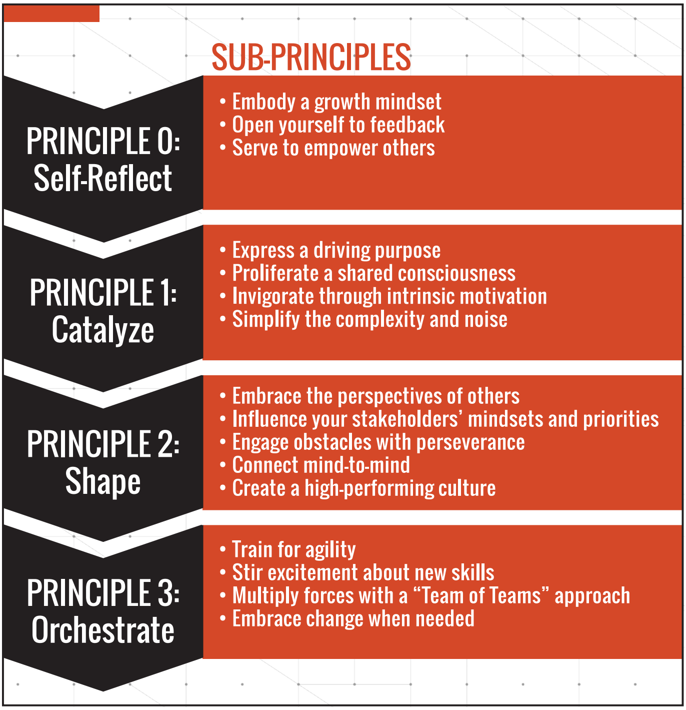

SUB-PRINCIPLES
PRINCIPLE 0: Self-Reflect
• Embody a growth mindset
• Open yourself to feedback
• Serve to empower others
PRINCIPLE 1: Catalyze
• Express a driving purpose
• Proliferate a shared consciousness
• Invigorate through intrinsic motivation
• Simplify the complexity and noise
PRINCIPLE 2: Shape
• Embrace the perspectives of others
• Influence your stakeholders' mindsets and priorities
• Engage obstacles with perseverance
• Connect mind-to-mind
• Create a high-performing culture
PRINCIPLE 3: Orchestrate
• Train for agility
• Stir excitement about new skills
• Multiply forces with a "Team of Teams" approach
• Embrace change when needed

Figure 2-1: Four key principles and their sub-principles for effective cyber leadership.

There are three sub-principles to self-reflection:

DON'T FORGET

1. **Embody a Growth Mindset**—Understanding that you are never finished learning, growing, and improving—and that it's okay if you aren't capable…yet. A growth mindset is about being comfortable with learning, stretching, and knowing that you'll need to acquire new skills throughout life.

2. **Open Yourself to Feedback**—Believing that other people hold critical perspectives and guidance that will help you grow. This belief is key to a growth mindset because it will help you view yourself as others see you, which is a valuable lens through which to assess your impact on the world around you.

3. **Serve to Empower Others**—Using your position as a leader to help others become their best selves. This is known as "Servant Leadership," a concept that promotes the idea of serving first and leading second. Rather than a command-and-control approach to leadership, Servant Leadership suggests you address the needs, expectations, and values of your team members first.

These three ideas will give you an excellent basis for becoming the kind of humble leader the cybersecurity world needs right now.

The Necessity of Catalyzing

Next we dive into "Principle 1: Catalyze," which looks at how to cultivate a vision and a following by employing psychology to grow, inspire, and align teams. This allows you to drive your cybersecurity program forward with both focus and intensity as your teams collectively strive to meet the needs of the business.

There are four key sub-principles that enable you to catalyze your teams:

DON'T FORGET

1. **Express a Driving Purpose**—Having a clear, concise, and compelling message of "here's what we're doing and why." We cannot overstate the critical importance of purpose, which several sub-principles directly support. Everyone needs to believe in and be excited by what they're doing.

2. **Proliferate a Shared Consciousness**—Creating a common worldview by making sure everyone knows and embraces the vision, mission, and purpose. A good example is the "Team of Teams" approach exemplified by the U.S. Joint Special Operations Command, in which siloes are broken down via communication that is transparent, clear, and frequent.

3. **Invigorate through Intrinsic Motivation**—Understanding what makes your key audiences tick, and use psychology to inspire them. Here we look at the importance of autonomy, mastery, and purpose to motivate team members to do their very best, stretch their limits, and contribute to the greater good.

4. **Simplify Complexity and Reduce Noise**—Making it easier for your team to focus, collaborate, and achieve. By simplifying as much as possible, you emphasize what's important, streamline operations, and drive better alignment on expectations. Cybersecurity is complex enough on its own; we don't need to make it any more complicated.

The Importance of Shaping

With "Principle 2: Shape," we learn how to influence business environments to enable tangible progress, turn obstacles into opportunities, and develop mental concordance with a wide range of important team members.

These skills will help you shape your internal and external environments to win hearts and minds and improve your odds of success. There are five sub-principles that enable you to shape the business environment within which your cybersecurity program operates:

DON'T FORGET

1. **Embrace the Perspectives of Others**—Practicing empathy and appreciation of "otherness." By striving to put yourself in the shoes of other people, you will better understand their worldview and what motivates their behavior.

2. **Influence Your Stakeholders' Mindsets and Priorities**—Being able to pull stakeholders to your point of view and managing change in ways that they'll embrace. This is important because shaping the environment requires influencing not just your team, but also key stakeholders outside the security program.

3. **Engage Obstacles with Perseverance**—Never giving up, even when it's hard. Brick walls are there to remind us of how badly we want something. By turning obstacles into opportunities through perception, action, and will, we can overcome almost anything that stands in our way.

4. **Connect Mind to Mind**—Thinking as one mind to accomplish bigger goals. This is done by developing a shared mental model, which creates synergy and ease around decisions and actions.

5. **Create a High-Performing Culture**—Developing active trust so team members can do their best work. Build an environment of safety among team members by ensuring a feeling of belonging and sharing personal vulnerabilities.

The Value of Orchestration

“Principle 3: Orchestrate” explains how to structure and choreograph resources to serve the business with the greatest agility and effectiveness. Through orchestration you can create a nimble and effective team, adapt quickly to today’s evolving cyber landscape, and ultimately lead in a way that raises the bar for performance.

There are four sub-principles that enable you to orchestrate as a leader:

DON’T FORGET

1. **Train for Agility—**Ensuring your team and the broader organization are both nimble and effective. Equanimity and flexibility when chaos or upheaval strikes are defining characteristics of a modern security program leader.
2. **Stir Excitement about New Skills—**Creating an environment that elicits the very best from your people. Be the kind of leader who accelerates team performance by empowering team members to test their unique skills and abilities, and challenging them to move out of their comfort zones.
3. **Multiply Forces with a “Team of Teams” Approach—**Developing a relational web within and among teams to create trust and collaboration. A team can be greater than the sum of its members only if they’ve developed trust and collaboration with each other and with people in other parts of the enterprise.
4. **Embrace Change When Needed—**Learning to adapt to evolving conditions. An effective leader helps the team weather stormy conditions with calm and composure by projecting confidence and offering reassurance.

Let’s dive in by looking at the value of self-reflection and how to get started.

Chapter 3

Principle 0: Self-Reflect

In this chapter

- Recognize that uncertainty will be a constant in your life
- Understand the value of life-long learning
- Establish an appreciation for how feedback helps you grow
- Embrace the importance of serving others

"By three methods we may learn wisdom: First, by reflection, which is noblest; Second, by imitation, which is easiest; and Third, by experience, which is bitterest."

— Confucius

In the last chapter we introduced the key principles for cyber leadership. Let's start with the foundation for all of these, which is the need to **self-reflect**. Becoming a true leader begins with a hard look inward. By seeking to know ourselves better, we can learn to gauge our interactions with the outside world and interpret how our actions affect those around us.

TIP

Only through self-reflection can we know our strengths and weaknesses, our truest intentions, and our deepest ambitions. By coming to terms with these realities, we can become our best selves. While most leadership books talk about the importance of being honest with your colleagues, I am advising you to start with yourself.

This chapter covers the importance of self-reflection and gives you three ways to accomplish it.

The Need for Self-Reflection

If you've ever been distracted (and who hasn't?), you know that human beings love to focus on things that are not critically important. We love the urgent, yet we procrastinate on the important. But in doing so, we miss out on our best chances to improve and potentially change the world in the process. Ray Dalio, author of *Principles*, explains: "Your unique power of reflectiveness—your ability to look at yourself, the world around you, and the relationship between you and the world—means that you can think deeply and weigh subtle things to come up with learning and wise choices."[2]

DON'T FORGET

There are three sub-principles that we previously touched on to help you self-reflect:

1. **Embody a Growth Mindset**—Understanding that you are never finished learning, growing, and improving.
2. **Open Yourself to Feedback**—Believing that other people hold critical perspectives and guidance that will help you grow.
3. **Serve to Empower Others**—Using your position as a leader to help others become their best selves.

Collectively, these concepts will help you establish the self-awareness and humility required to lead others in this technology-dependent, ever-changing world. Let's dive in.

1. Embody a growth mindset

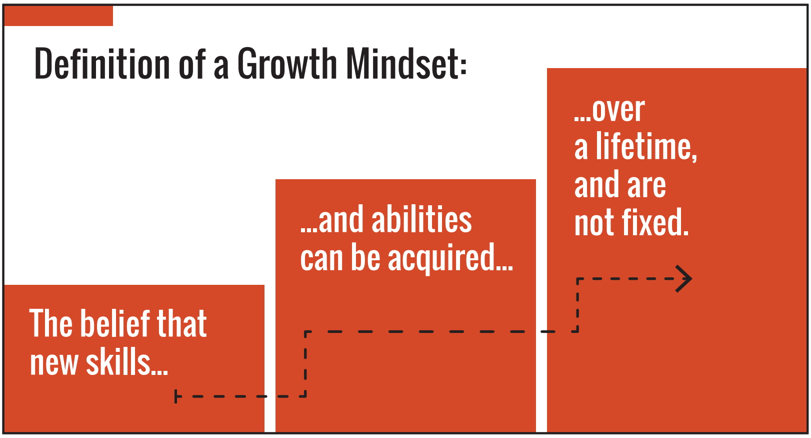
"I am always doing what I cannot do yet in order to learn how to do it." – Vincent Van Gogh

With the world evolving at such an overwhelmingly rapid pace, it's understandable to hope we might be exempt from evolving with it. Many people believe that they are somehow immune to change; this is known as a fixed mindset. A **growth mindset**, on the other hand, is the belief that new abilities can and should be acquired. The idea is, if you feel incapable of something, it just means you're not capable...yet.

[2] Ray Dalio, *Principles* (Simon & Schuster, 2017), 152.

Both people and organizations have mindsets, according to Carol Dweck, author of *Mindset: The New Psychology of Success*. She says: "An organization might embody a fixed mindset, conveying that employees either 'have it' or they don't: We call this a 'culture of genius.' Or it might embody more of a growth mindset, conveying that people can grow and improve with effort, good strategies, and good mentoring. We call this a 'culture of development.'"[3]

Think about that for a moment: which organization would you rather work for? If you answered, "culture of development," you're not alone. Dweck notes, "People who work in growth-mindset organizations have far more trust in their company and a much greater sense of empowerment, ownership, and commitment."[4] And "Supervisors in growth-mindset companies saw their team members as having far greater management potential than did supervisors in fixed-mindset companies. They saw future leaders in the making."[5]



Definition of a Growth Mindset:

The belief that new skills...

...and abilities can be acquired...

...over a lifetime, and are not fixed.

Figure 3-1: What does a Growth Mindset really mean?

[3] Carol S. Dweck, Ph.D., ***Mindset: The New Psychology of Success*** (Ballantine Books, 2016), 142.

[4] Ibid., 143.

[5] Ibid., 144.

Embodying a growth mindset in cybersecurity

TIP

If you're far enough along in your career, you might think you've experienced it all. But I hope you don't believe that. Instead, if you've adopted a growth mindset, you know you have a lot to learn. Ask:

- ☑ What aspects of our business are changing? What impact does that change have on cybersecurity?
- ☑ How do new business technology investments change our approach for delivering cybersecurity?
- ☑ What types of benefits would attract the next generation of cyber talent to work here?
- ☑ What must I do to help the organization understand and adapt to an evolving cyber threat landscape?
- ☑ What important leadership skills must I develop to maximize my team's outputs and fulfillment?
- ☑ What are some creative ways we could use to break down barriers to our success?

Example answers might include:

- ☑ With our acquisition-focused growth strategy, we'll need to understand the nuanced risks that these acquisitions present to our business, and protect accordingly.
- ☑ The rapid move to PaaS and SaaS cloud computing will really test our ability to securely manage identities and access.
- ☑ The millennial workforce is looking for leadership that appreciates today's "results-oriented economy" and allows for significant flexibility in doing the job.
- ☑ Getting organizational buy-in on this new security initiative will require some alliance building with a select set of business units and individuals within our company.

Skills to develop

If "not knowing" makes you uncomfortable, it's time for a reckoning. The fact is, you and your team will always be at a knowledge disadvantage in some way or another, and I'm not just talking about cyber threat activity. You'll generally be grasping for knowledge every day in technical, political, and cultural arenas. But don't stress. The key is to know your critical gaps, set your goals for closing them, and develop a systematic path towards improvement. You'll adjust your path as you learn more, and that's okay. Here are some tactics for embracing this reality and living a growth mindset:

- Regarding critical needs, identify your unknowns and make a prioritized plan on how to acquire that knowledge.
- Every day, write down important questions that you want answered. Maybe they're the same questions as the day before, but use them as a tool for bringing focus to your life and that of the team.
- Encourage your team to explore challenges and become obsessive about learning; reward learning that drives action.
- Be open minded about areas for improvement—everything is on the table—and be honest about why and what you want to improve.
- Incentivize others for constructively challenging the status quo and asking tough questions that seek to find a better way.

CAUTION

Dweck cautions some latitude: "The growth mindset is the belief that abilities can be cultivated. But it doesn't tell you how much change is possible or how long change will take. And it doesn't mean that everything, like preferences or values, can be changed....The growth mindset also doesn't mean that everything that can be changed should be changed. We all need to accept some of our imperfections, especially the ones that don't really harm our lives or the lives of others."[6]

In additional to lifelong learning and the belief that you can improve through skill acquisition, opening yourself to feedback is a critical puzzle piece to effective self-reflection.

[6] Ibid., 50.

2. Open yourself to feedback

"There is no failure. Only feedback." – Robert Allen

One of the ways to maintain a growth mindset is to open yourself to feedback. Dalio pairs being open-minded with receiving better feedback. He says: "The more open minded you are, the less likely you are to deceive yourself—and the more likely it is that others will give you honest feedback...It can also be difficult because being radically transparent rather than more guarded exposes one to criticism. It's natural to fear that. Yet if you don't put yourself out there with your radical transparency, you won't learn."[7]

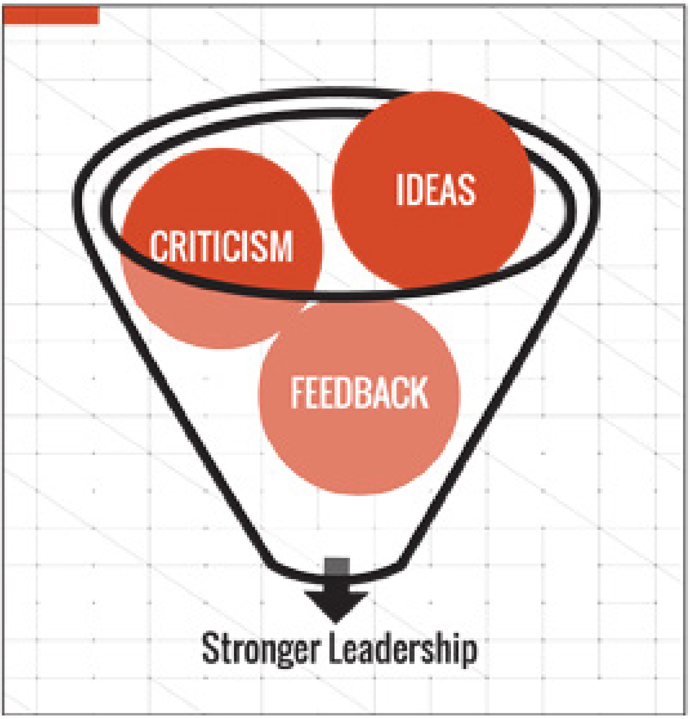


Figure 3-2: You become a stronger leader when you are open to all feedback, not just what you want to hear.

[7] Dalio, *Principles*, 136.

Honest feedback is critical in learning—understanding what is happening and seeing how things truly are, even when they aren't going to plan. Dalio explains: "There is no avoiding pain, especially if you are going after ambitious goals. Believe it or not, you are lucky to feel that kind of pain if you approach it correctly, because it is a signal that you need to find solutions so you can progress. If you can develop a reflexive reaction to psychic pain that causes you to reflect on it rather than avoid it, it will lead to your rapid learning/evolving."[8]

How feedback strengthens cyber leadership

TIP

When you show your team that they can be honest with you, they will relax and stop telling you what they think you want to hear. They'll instead tell you what you need to hear. This keeps the lines of communications open and keeps you in the position of receiving the most pertinent information to make the best decisions. Ask your teams:

- ☑ How can I improve? What can we do to improve?
- ☑ Where are we falling short? What's going well that should be recognized?
- ☑ What have you learned that should be shared with the team?
- ☑ What are our blind spots? What could hurt us down the road?
- ☑ Where are we lacking in transparency or clarity?
- ☑ How can we better re-balance our capability investments to address risk?

[8] Ibid., 136.

Skills to develop

Opening yourself to feedback—and constructively providing it to others—requires habit-forming repetition. In *Principles*, Dalio expounds at length on the value of radical transparency as the everyday norm. To start down this path yourself, begin here:

- Build feedback into your operational processes—embed team after-action reviews and one-on-one coaching as cultural norms so that giving or receiving them isn't seen as a "special" activity.
- Realize that most people are coming from a good place with their feedback; even when the message stings, it's usually meant to help. Try to see the good.
- Develop your active listening skills: listen to understand, not to respond.
- Identify and document your areas of strength and weakness by learning from your colleagues (and friends/family), not just relying on your self-perception.
- Solicit feedback regularly from a range of stakeholders that you respect, even those that you have loose contact with; everyone's perspective has potential value.

A growth mindset and willingness to receive feedback will help you better serve your teams, which is our third concept. Let's take a look.

3. Serve to empower others

"The best way to find yourself is to lose yourself in the service of others." – Mahatma Gandhi

If you've been promoted to your position, it's likely because you were of service to the company and its people. A well-known concept called Servant Leadership was first promulgated by Robert Greenleaf in the 1970s. He says, "A new moral principle is emerging which holds that the only authority deserving one's allegiance is that which is freely and knowingly granted by the led to the leader in response to, and in proportion to, the clearly evident servant stature of the leader...To the extent that this principle prevails in the future, the only truly viable institutions will be those that are predominantly servant led."[9]

[9] Robert K. Greenleaf, *Servant Leadership: A Journey into the Nature of Legitimate Power and Greatness* (Paulist Press, 1977), 10.

This idea is as pertinent today as it was then. Greenleaf states, “The servant-leader *is* servant first...It begins with the natural feeling that one wants to serve, to serve *first*. Then conscious choice brings one to aspire to lead. That person is sharply different from one who is a *leader* first, perhaps because of the need to assuage an unusual power drive or to acquire material possessions. For such it will be a later choice to serve—after leadership is established.”[10]

Dalio expounds upon this idea: “You will have to decide to what extent you will put the interests of others above your own, and which others you will choose to do so for. That’s because you will regularly encounter situations that will force you to make such choices.”[11]

Empowering others as a cyber leader

TIP

Rather than leading by “command and control,” how can you better serve your teams? In other words, how can you put yourself in the service of your team and company—and how can you be of greater service so that your teams feel empowered to do their best? This is all about maximizing their potential and wanting them to be a part of your program. We’ll look at the concept of autonomy in the next chapter, but for now, consider:

> ☑ Putting a lot of detailed thinking into cybersecurity governance—providing a distributed set of decision rights (and therefore autonomy) to a range of highly skilled, yet trustworthy, individuals. Not only does this empower and inspire those people, but it also increases the speed and agility of the organization overall.
>
> ☑ Advocating for your team’s needs based on their input and feedback. For example, loosening rules and requirements, and giving them more latitude.
>
> ☑ Encouraging and rewarding others to speak up publicly to report anything that is not working properly, such as team dynamics, processes, expectations, culture, and tasks, among other things. Ensure that you follow up and report regular progress.

[10] Ibid., 13.

[11] Dalio, *Principles*, 150.

☑ Coaching and mentoring high-potential individuals within your program. Let them sit in on executive-level meetings, give them "stretch" tasks that challenge their way of operating, and so on. A good leader is always growing their replacement.

Skills to develop

In the long run, serving others first (before yourself) will produce the team results and self-fulfillment that you seek. Operating in this way requires real emotional intelligence and "soft" skills—skills that have long been neglected in the cybersecurity arena. It's time to collectively up our game in this area. Here's how:

- Practice empathy, and constantly communicate the need for team members to envision a situation from another's point of view.
- Develop your coaching skills and practice them daily.
- Look at how you can become a better negotiator on behalf of your team—understand how to gather the right inputs and methodically drive toward the outcomes (e.g., funding access, technology decision making) that your people need.
- Examine whether your goals are in alignment with your team's goals and what you can do to bring them closer together.

Greenleaf eloquently sums up the value and intent of servant leadership: "When the business manager who is fully committed to this ethic is asked, "What are you in business for?" the answer may be: "*I am in the business of growing people*—people who are stronger, healthier, more autonomous, more self-reliant, more competent."[12]

We'll look more closely at that idea in the next chapter, "Principle 1: Catalyze," and see what it means to cultivate a vision and a following. This discussion includes four subprinciples that will help you inspire teams.

[12] Greenleaf, *Servant Leadership: A Journey into the Nature of Legitimate Power and Greatness*, 147.

Chapter 4

Principle 1: Catalyze

In this chapter

- **Learn how to cultivate a vision and a following**
- **Employ psychology to inspire, grow, and align teams**
- **Drive your program forward with resolute focus and intensity**

"The key to successful leadership today is influence, not authority."

– Ken Blanchard

Time and again we hear stories of companies and leaders unable to inspire their teams. Why is that? Because they have not learned how to **catalyze**. By this, I mean to cultivate a vision and a core following around it. The leader is the catalyst, bringing to life an idea that intrigues and inspires people—and compels them to get on board.

When you are unable to catalyze, you are left with misaligned, siloed groups of professionals following their own goals in their own way. Cultural microcosms pop up, many of which are unfulfilling. Unfortunately, this situation is extremely common in the cybersecurity field. Not only does it prevent you from achieving your desired results as the leader, it also paves the way for disenfranchised team members and a negative work environment.

This chapter covers how to catalyze your teams by casting an inspiring idea of the future and rallying a devoted cadre.

The Need to Catalyze

Great leaders who can catalyze their teams create loyal members that inevitably stretch to new heights. That's because people work for people, not companies, and employees who are happy with their leaders tend to stay, become more productive, and achieve results.

There are four key sub-principles we've introduced earlier that enable you to catalyze your teams:

DON'T FORGET

1. **Express a Driving Purpose**—Having a clear, concise, and compelling message of "here's what we're doing and why."
2. **Proliferate a Shared Consciousness—**Creating a shared worldview where everyone knows and embraces the vision, mission, and purpose.
3. **Invigorate through Intrinsic Motivation—** Understanding what makes your key audiences tick, and using that knowledge to inspire them.
4. **Simplify the Complexity and Reduce Noise—**Making it easier for your team to focus, collaborate, and achieve.

Taken together, these four sub-principles reinforce each other for the best outcomes. Let's take a closer look.

1. Express a driving purpose

"He who has a why to live for can bear almost any how."
– Friedrich Nietzsche

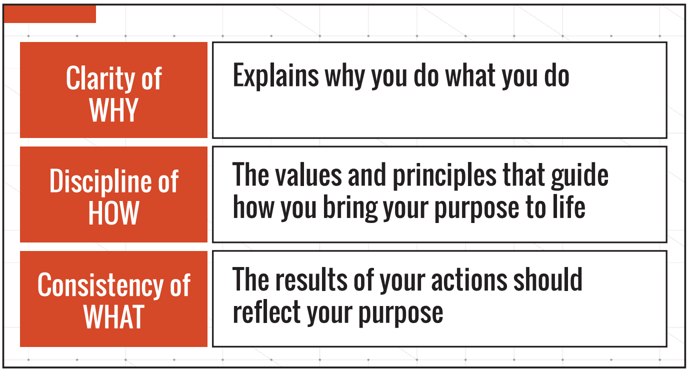
In order to catalyze your team, you first must design and express a vision of what you want to accomplish and, most importantly, **why**. People seek a greater purpose to inspire them, and the best way to inspire, according to Simon Sinek, author of *Start With Why: How Great Leaders Inspire Everyone to Take Action*, is to ask: "Why does your organization exist? Why does it do the things it does?...Why are people loyal to some leaders, but not others?"[13]

[13] Simon Sinek, *Start with Why: How Great Leaders Inspire Everyone to Take Action* (Penguin Group, 2009), inside front cover.

As the leader, your answer should have nothing to do with time to detect or contain a cyber threat, or percentage of vulnerabilities managed—those are outcomes. Instead, the leader's job is to nurture an environment that promises something much more fulfilling. What people need is a leader that embodies an exciting, aspirational vision that pulls people in like a gravitational force. This is your driving purpose. Sinek explains: "If we were all rational, there would be no small businesses, there would be no exploration, there would be very little innovation and there would be no great leaders to inspire all those things. It is the undying belief in something bigger and better that drives that kind of behavior."[14]

He goes on to describe what you must do, and in what order, to express your driving purpose. Specifically, you must have the:

DON'T FORGET



Clarity of WHY	Explains why you do what you do
Discipline of HOW	The values and principles that guide how you bring your purpose to life
Consistency of WHAT	The results of your actions should reflect your purpose

Figure 4-1: Three elements necessary to express a driving purpose.

This creates an environment where people are excited to come to work. Sinek says: "Great organizations become great because the people inside the organization feel protected. The strong sense of culture creates a sense of belonging and acts like a net. People come to work knowing that their bosses, colleagues and the organization as a whole will look out for them. This results in reciprocal behavior. Individual decisions, efforts and behaviors that support, benefit and protect the long-term interest of the organization as a whole."[15]

[14] Ibid., 62.
[15] Ibid., 105.

Finding your cyber why

TIP

So how does expressing your driving purpose apply to cybersecurity? The most important step is to ensure you have uncovered and communicated the core values, attitudes, and beliefs necessary for better cybersecurity. Ask:

- ☑ What difference are we trying to make in this company? In the world?
- ☑ Why is this important to our organization?
- ☑ How can we best express this belief through our work?
- ☑ What opportunities do we have to educate and enlighten others—both inside and outside our organization?
- ☑ How can we grow as unique individuals here versus another company?

Example answers might include:

- ☑ Our company's societal value hinges on connecting people globally through technology, and we want to make sure we have the right protections in place.
- ☑ Our children will depend on the secure operations of IoT, and since we're a maker of IoT products and services, we have a commitment to generations of people going forward to get this right.
- ☑ We have unique knowledge about a potentially existential risk type—it's our duty to enlighten our colleagues so that they learn how to help manage it.
- ☑ What opportunities do we have to educate and enlighten others—both inside and outside our organization?
- ☑ The community here embraces individual growth and opportunity. We want our team members to say: "I can find real happiness here, develop a broad array of useful skills, and build impactful relationships across this company."

Skills to develop

As you go about finding your cyber why, you'll want to:

- Regularly ask your team, "Why do you do what you do?" and "Why does the company do what it does?" Be sure that the answers are aligned with the driving purpose you want to see expressed in your business culture.
- Hire for mindset first, and skillset second. In other words, hire for why, not solely just for what.
- Ideate with your team on what the "big picture" looks like; have them feel that they are part of the "why" the security program exists in the first place.
- Define a simple yet powerful vision that speaks to the hearts and minds of the audiences you seek to influence.

We've seen the importance of purpose, but what's the best way to communicate it throughout the organization? That's where transparency comes in. Let's take a look.

2. Proliferate a shared consciousness

"A lack of transparency results in distrust and a deep sense of insecurity." — Dalai Lama

I've seen many companies, particularly as they grow, divide into siloed departments (either unintentionally or on purpose) where cross-communication and information sharing is negligible. The danger of this is that when teams don't have the information they need to do their jobs properly, collaboration comes to a standstill and decision making begins to stall.

The second component to catalyze your team, then, is to think as one mind, where everyone knows the vision, mission, and purpose. This is done through implementing measures of massive transparency, and ensuring your team members and other relevant stakeholders have reasonably deep visibility into every part of the security program, combined with communications up, down, and across the organization. In this way, you move from a disjointed, out-of-synch, siloed organization toward one cohesive unit that employs a **shared**

consciousness.

This approach is best described by General Stanley McChrystal in his book, *Team of Teams: New Rules of Engagement for a Complex World*, in which he talks about restructuring the Joint Special Operations Task Force "from the ground up on principles of extremely transparent information sharing (what we call 'shared consciousness') and decentralized decision-making authority ('empowered execution')."[16]

What this means is that information is not kept in a locked vault to enhance someone's power position; it is freely shared across the organization in order to help team members make better decisions based on a more comprehensive understanding of the situation. McChrystal elaborates: "The relationship between context and authority is as ancient as it is intuitive, but it has usually been directed by improving the information given to senior leaders, thereby enhancing their decision-making purview…We reversed this direction. We used shared consciousness to pump information out, empowering people at all levels, and we redefined the role of leaders…."[17]

So rather than moving information solely up the ladder, consider how you can share information in every direction to give your teams the context they need to make the best decisions.

[16] General Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (Penguin Publishing Group, 2015), 20.

[17] Ibid., 246.

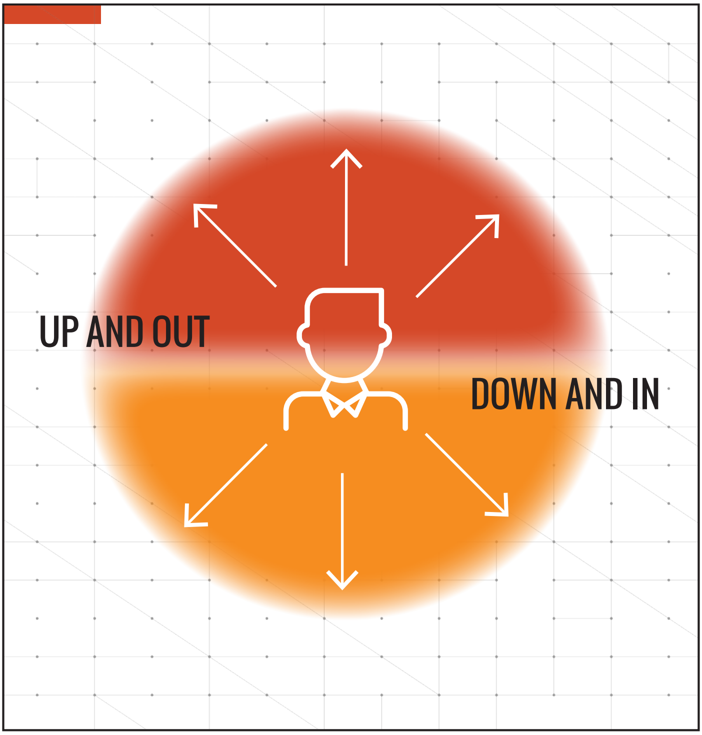


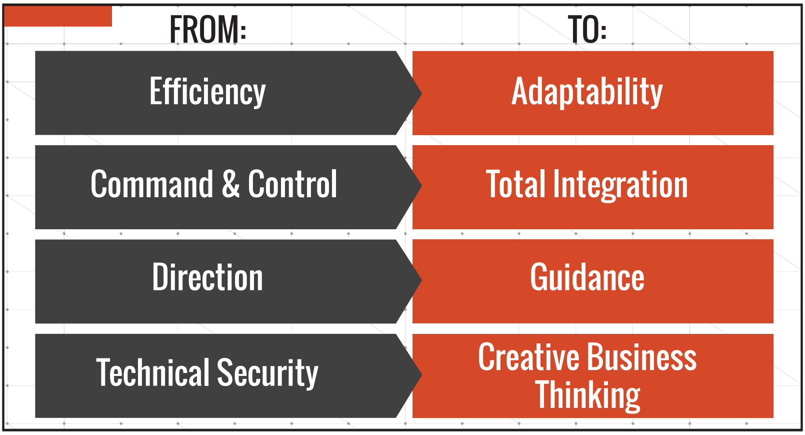
Figure 4-2: Shared consciousness means access to information at all levels for better decision-making.

How shared consciousness applies to cybersecurity

TIP

Cybersecurity needs to be one fight, one team. Having multiple functional teams operate in their own worlds, each with their own belief system and worldview, is a difficult way to function. It's often ineffective and inefficient. Instead, fusing together various functional teams—threat intelligence, detection, response, risk management, stakeholder engagement, and so on—under a single construct can bring newfound levels of productivity and improved culture. And doing so informs the "science"—the right security architecture and tooling. Getting there all starts with establishing a shared consciousness—the connective tissue that binds the various teams to think and act as one.

I talked about this very principle in an article I wrote for Dark Reading with Gary Barnabo: “We’re at a tipping point for how cybersecurity organizations must look and operate to protect and enable the business. Efficiency must give way to adaptability. Command and control to autonomy. Direction to guidance. Collaboration to total integration. Technical security experts aren’t enough; these assets must be blended with creative business thinkers who understand how security investments should relate to enterprise strategy and risk.”[18]



FROM:	TO:
Efficiency	Adaptability
Command & Control	Total Integration
Direction	Guidance
Technical Security	Creative Business Thinking

Figure 4-3: How cybersecurity organizations must operate to protect and enable the business.

That’s what happens when it’s the leader’s job to ensure people have the most up-to-date data—the organization can evolve to a more agile, fluid structure; one that is better positioned to tackle the onslaught of today’s cyber threats.

Lastly, this transparent way of operating needs to pervade throughout the broader ecosystem that your security program operates within. It’s not enough to only look “down and in” when bringing your program into alignment. Likewise, it’s equally important to engage “up and out”—keeping senior peers, executives, and key external partners (such as cloud providers, suppliers, customers, etc.) “in the know” about

[18] Matthew Doan and Gary Barnabo, “The Team of Teams Model for Cybersecurity,” Dark Reading, September 12, 2017. https://www.darkreading.com/application-security/the-team-of-teams-model-for-cybersecurity/a/d-id/1329840?piddl_msgorder=asc.

what's happening and what your needs are. With today's expansive attack surface, broad transparency is vital (see Figure 4-2).

Skills to develop

In transitioning to a mode of pervasive transparency and open communications, it's important to:

- Learn to communicate internally with all levels of the company and externally with key business partners.
- Socialize the established vision again and again. Clarify for your audience how changes to that vision directly impact them, and ask for feedback so that they embrace the vision as their own.
- Work on interpersonal skills, approachability, effective listening skills, and appropriate use of style and language for the specific audience with whom you're communicating.
- Practice empathy such that you understand the challenges facing your audiences and can speak to how to address them.
- Build an emotionally intelligent leadership group around you; one that can model the behaviors you seek to portray.

Even with massive transparency and shared communications, your teams still need to be motivated. Let's look at how to support that.

3. Invigorate through intrinsic motivation

"I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel." – Maya Angelou

You've expressed your driving purpose and aligned your teams behind these beliefs with a shared consciousness through transparency, visibility, and communications. Now it's time to motivate. No one knows this better than Daniel H. Pink, author of *Drive: The Surprising Truth About What Motivates Us*. He says: "When it comes to motivation, there's a gap between what science knows and what business does. Our current business operating system—which is built around external, carrot-and-stick motivators—doesn't work and often does harm. We need an upgrade. And the research shows the way. This new approach has three essential elements:

DON'T FORGET

1. **Autonomy:** the desire to direct our own lives.
2. **Mastery:** the urge to get better and better at something that matters.
3. **Purpose:** the yearning to do what we do in the service of something larger than ourselves."[19]

Let's look at each in more depth:

Autonomy

An environment that gives its workers autonomy focuses on results instead of rules, giving them the freedom to find the best way, reinvent processes, and suggest new ones. In this way, autonomy provides an environment for people to do their best work.

CAUTION

Don't confuse autonomy with complete independence. Team members are still responsible for their individual roles, and must collaborate well with others. All told, autonomy in business goes a long way to providing team members with an environment in which they can flourish.

Mastery

The desire to master a skill takes people from compliance, where they are just following the rules, to engagement, where work becomes more like play. Research shows that engagement is one of the best predictors of productivity. Pink notes that mastery is a mindset, a concept we delved into in the prior chapter, and that it can be painful (think about when you've learned a new sport and you can understand why), and that it's impossible to fully realize. Simply put, mastery is a never-ending process, but the journey towards it is incredibly rewarding.

[19] Daniel H. Pink, ***Drive: The Surprising Truth About What Motivates Us*** (Riverhead Books, 2009), 219.

Purpose

I love that purpose is the third piece of the motivation triad, as we've already explained why it's so important earlier in this chapter. Pink says it best: "Autonomous people working toward mastery perform at very high levels. But those who do so in the service of some greater objective can achieve even more. The most deeply motivated people—not to mention those who are most productive and satisfied—hitch their desires to a cause larger than themselves."[20]

Motivating as a cyber leader

TIP

We know that much of the daily routine in security can be monotonous—triaging alerts, prioritizing, and figuring out which events to follow up on and how. Rather than throwing a 90-page cookie-cutter incident response playbook at your seasoned team, how about giving them the latitude and flexibility to do what they believe is appropriate? Give them a guiding construct, but let them infuse real-time context to guide exactly how they'll respond. Here are some ways to do that:

☑ Make mastery cool: reward it publicly and inspire people to strive for it.

☑ Remind people of the higher purpose they're serving and the larger implications of their work. Yes, cyber is carried out in the interest of the business. But, for example, it can loom much larger than that when it comes to critical infrastructure, national security, and the safety of future generations.

☑ Crowdsource ideas for strategic security initiatives throughout all levels of the organization.

☑ As the leader, remember that you are a servant of your teams, as we learned in the last chapter. So, act as one of the team members, even if it means blood, sweat, and tears.

[20] Ibid., 131.

Skills to develop

In motivating your teams, look at how you can help them become autonomous, master new skills that matter, and do work that has significant meaning to a wide audience.

- Visibly empower proven individuals with decision rights, and push that power down to the lowest layers of authority possible, especially if you are working in a complex/large organization.
- Cultivate a sense of community where working with one another collaboratively is the norm. Good ideas only become great as you test and socialize them across the organization.
- Establish open forums to have "straight talks" about what is and is not working within the security program. Test, fail, and learn as a unit. Level-set with your teams to ensure that they're accountable for results.

Lastly, let's look at how to streamline these concepts.

4. Simplify complexity and reduce noise

"Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it's worth it in the end because once you get there, you can move mountains." — Steve Jobs

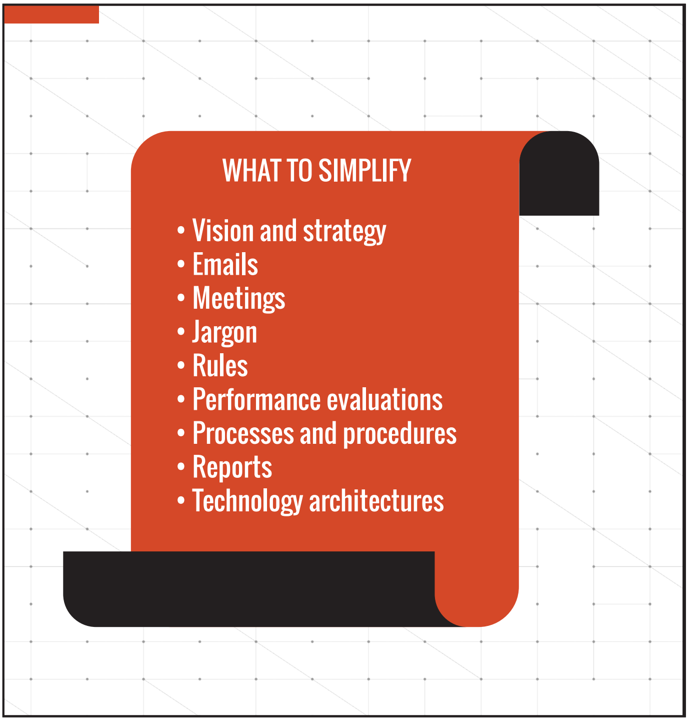
I urge you to simplify...greatly. Complexity is the enemy of leadership—and security—in almost every way imaginable. "Embracing the fact that success or failure in this space is based on how well we all do the simple, small things is where the difference is made. Simplicity is a strategy, and it works."[21]

One of the most well-known drivers of simplicity in business is Lisa Bodell, author of *Why Simple Wins*, in which she notes "Complexity is killing companies' ability to innovate and adapt, and simplicity is fast becoming the competitive advantage of our time. By learning how to cut out redundancies, communicate with clarity, and make simplification a habit, individuals and companies can begin to recognize which

[21] Chase Cunningham, "Simplicity is a Strategy that Works," Forrester Blog on Privacy, Security and Risk, June 19, 2017. https://go.forrester.com/blogs/17-06-19-simplicity_is_a_strategy_that_works/.

activities waste our time and which create lasting value. As low-value work disappears, individuals feel less overwhelmed, more empowered, and more able to spend each day doing things that matter."[22]

Ideally, you need to make simplification something that happens routinely and continually. What should you simplify? Everything! For example:



WHAT TO SIMPLIFY

- Vision and strategy
- Emails
- Meetings
- Jargon
- Rules
- Performance evaluations
- Processes and procedures
- Reports
- Technology architectures

Figure 4-4: Some of the many things you can simplify.

Bodell notes that something that's properly simplified is as minimal as possible, as understandable as possible, as repeatable as possible, and as accessible as possible. She suggests that you make the lives of others as simple as possible, just as you'd like them to do for you. I suggest you make that your mantra.

[22] Lisa Bodell, *Why Simple Wins: Escape the Complexity Trap and Get to Work that Matters* (Bibliomotion, 2017), xiv.

Simplifying as a cyber leader

Cybersecurity is anything but simple, but unfortunately "complexity is the worst enemy of security," according to Bruce Schneier. Instead, you can maximize positive impact by getting the basics right, making complex procedures and reporting easier, and streamlining how your organization operates. Here are some ideas:

☑ Everyone around you (360 degrees) needs to understand the why, how, and what of your work as simply as possible. So do the hard, upfront legwork to ensure your message truly resonates.

☑ Don't accept that something is inherently complex; figure out how to simplify even complicated tasks, structures, and rules. If Steve Jobs did it, so can you.

☑ Cyber-related data (e.g., event logs) can be overwhelming and hard to use. Instill a guiding principle within people to fine-tune processes and tools until it's easy to see the signal in the noise.

Skills to develop

Simplicity gives people comfort that the security program is confident and thriving, and that will encourage people to invest their energy into it. You would be wise to:

- Build simplicity into processes and make simplification a core value.
- Employ the "five whys" technique from the Toyota Production System.[23] For every identified problem, drill down to the root cause by asking "why?" five times for every single challenge.
- Distill complexity down to its simplest form in every case. You'll see that this skill is an invaluable art form that greatly enables your program.
- Identify and empower skilled "simplicity" talent on your team to help you, as the leader, translate the complex (e.g., cyber risk scenarios) into easily understood messages that stakeholders can connect with (e.g., stories and analogies).
- Make "going simple" a fun activity; stretch your scientists to become artists in simplicity.

[23] Taiichi Ohno, "Ask 'why' five times about every matter," Toyota Traditions, March/April 2006. http://www.toyota-global.com/company/toyota_traditions/quality/mar_apr_2006.html

In the next chapter, “Principle 2: Shape” we’ll look at what it means to convert hearts, minds, and conditions in the business environment to engender the security program’s success.

Chapter 5

Principle 2: Shape

In this chapter

- Shape environmental conditions to engender success
- See hard challenges as breakthrough opportunities
- Develop mental concordance across your extended team

"No matter how much internal resolve you have, you will fail to change your life if you don't change your environment."

– Benjamin Hardy

In the previous chapter, we learned how to inspire and motivate teams, but what about shaping their surrounding environment to enable success?

Great leaders influence their surroundings by **shaping** not only the values, expectations, and behavior of their teams, but also those of the organization as a whole.

What does it take to be a shaper? Dalio says it best: "I've found that shapers tend to share attributes such as intense curiosity and a compulsive need to make sense of things, independent thinking that verges on rebelliousness, a need to dream big and unconventionally, a practicality and determination to push through all obstacles to achieve their goals, and a knowledge of their own and others' weaknesses and strengths so they can orchestrate teams to achieve them."[24]

[24] Ray Dalio, *Principles,* 230.

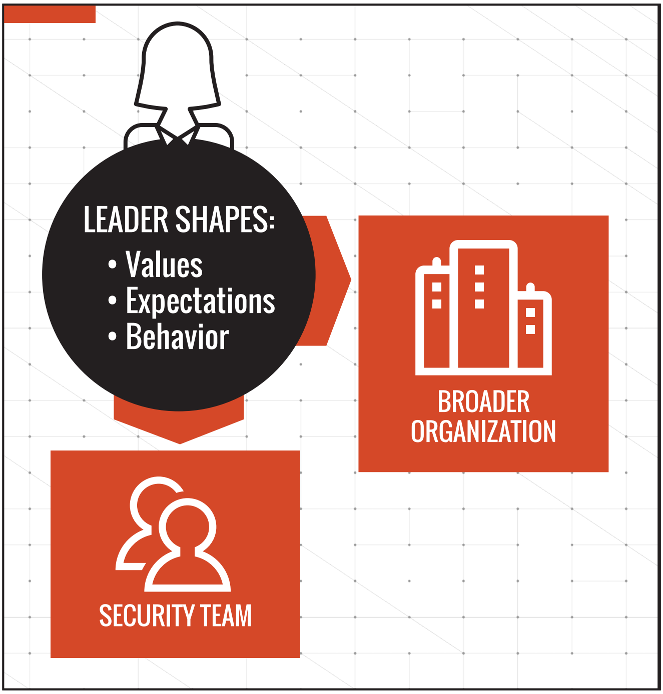


Figure 5-1: Great leaders shape not just their teams, but also the organization as a whole.

TIP

This mindset will enable you to evolve your leadership skills from looking “down and in” at your program, to looking “up and out.” You need to influence key stakeholders and shape environmental conditions in a way that improves your odds of success. This is vital in cybersecurity, as real progress only comes about when key individuals and organizations outside of the security program start embracing and contributing to the cyber mission.

No cyber leader can achieve a successful program through willpower alone; the mission is too complex and interdependent for that. You need to influence others’ priorities and shape their behaviors to facilitate your goals.

To that end, this chapter covers how to shape environmental conditions so that: 1) cybersecurity becomes part of the company’s cultural DNA; and 2) your team is on board and excited to execute the mission.

The Need to Shape

The environment you create influences the outcomes you achieve. As a cyber leader, you need to establish an enriched environment because relying on willpower alone to get the job done will likely fail.

Envisioning this enriched environment and taking steps toward creating it are critical to the groundwork for making material cybersecurity change happen. This will help you shape the mindsets and incentive structures of key internal and external stakeholders so that they want to make the choices that you desire.

Proper shaping will make your efforts stick and endure for the long term. I'm stating the obvious here, but I trust you're in the business of creating something durable and meaningful.

I've highlighted the five key sub-principles that enable you to shape the business environment within which your cybersecurity program operates:

DON'T FORGET

1. **Embrace the Perspectives of Others**—Practicing empathy and appreciating "otherness."
2. **Influence Your Stakeholders' Mindsets and Priorities**—Being able to orient stakeholders to your point of view and managing change so that they'll embrace it.
3. **Engage Obstacles with Perseverance**—For things that matter, never giving up, even when it's hard. Brick walls are there to remind us of how badly we want something.
4. **Connect Mind-to-Mind**—Employing similar decision processes and behaviors across the team in an effort to accomplish bigger goals.
5. **Create a High-Performing Culture**—Developing an atmosphere of belonging and trust so team members can do their best work.

Let's see how these sub-principles work together.

1. Embrace the perspectives of others

“No one cares how much you know, until they know how much you care.” – Theodore Roosevelt

Being open to other people’s perspectives enables us to **practice empathy**. And in learning what other people value and how they think, we can better shape the environmental conditions for their success.

According to the authors of *Neuroscience for Leadership*, “Empathy is not just the ability to understand that others have emotions and feelings and to feel some concern or distress about them as a result, but the ability to feel as they do (or nearly as they do), to ‘take a step in their shoes.’ Empathy is a precursor to behavior that is beneficial to others—known as prosocial behavior.”[25]

Adam Grant, author of *Give and Take: A Revolutionary Approach to Success*, explains: “When we empathize with a person, we focus our energy and attention on helping him or her—not because it will make us feel good but because we genuinely care.”[26]

To learn how to practice empathy and embrace the perspectives of others, the authors of *Neuroscience for Leadership* offer these suggestions:

> ☑ “Try to put yourself in the shoes of others—what is their raison d’être?
>
> ☑ Which factors motivate and de-motivate yourself and others?
>
> ☑ How can knowing about this help you work better with your team?
>
> ☑ How can knowing yourself better help you achieve purpose and meaning at work, as a leader and in life?”[27]

[25] Tara Swart, Kitty Chisholm, and Paul Brown, *Neuroscience for Leadership: Harnessing the Brain Gain Advantage* (Palgrave MacMillan, 2015), 80.

[26] Adam Grant, *Give and Take: A Revolutionary Approach to Success* (Viking, Penguin Group, 2013), 220.

[27] Swart, Chisholm, and Brown, *Neuroscience for Leadership: Harnessing the Brain Gain Advantage*, 143.

Dalio notes, “Recognize that to gain the perspective that comes from seeing things through another’s eyes, you must suspend judgment for a time—only by empathizing can you properly evaluate another point of view. Open-mindedness doesn’t mean going along with what you don’t believe in; it means considering the reasoning of others instead of stubbornly and illogically holding on to your own point of view.”[28]

Empathizing as a cyber leader

TIP

How can you embrace the perspectives of others at work and empathize with them? Listening is key—not to respond but to understand. That means not judging or interjecting your opinion, but rather, asking open-ended questions to ensure you understand the big picture. Only then can you give people what they really need: compassion, time, guidance, budget, or other resources.

Think about how you can better understand what matters to your team members and stakeholders to create an environment in which individuals flourish and you’re executing the mission in the right way. Here is data you might gather in seeking to understand the viewpoints of others:

- ☑ What business leaders think about when they hear “cybersecurity”
- ☑ The top pressures (and goals) being placed upon business units and shared service organizations
- ☑ Strategic cost-cutting measures being implemented across the company
- ☑ The aspirations of your high-potential team members, no matter where they sit in the program

[28] Dalio, *Principles,* 189.

Skills to develop

Time and again, I see people in leadership positions who aren't leading. Instead, they're managing from a very senior position. One of the biggest shifts from managing to leading involves embracing the perspectives of others. Start here:

- Realize that your opinion isn't the only one; your team members have valuable points of view that you might not have considered.
- In empathizing with others, learn to balance taking with giving, but don't give so much that you burn out.
- If you're naturally empathetic, make sure that you're seeing and evaluating the outcomes of the energy you expend.
- Don't jump to conclusions about the meaning of someone else's communication until they've fully stated their case.
- Be extremely careful with your precious time, making sure you're spending it with the right people for the right reasons.

Embracing the perspectives of other people is a key to being influential, particularly when it comes to stakeholders. Let's take a look.

2. Influence stakeholders' mindsets and priorities

"Persuasion skills exert a far greater influence over others' behaviors than formal power structures do."
– Robert Cialdini

Part of shaping the environment is influencing not just your team, but also the key stakeholders outside of the security program—all of whom have their own priorities and mindsets.

You need them to understand and support the cybersecurity mission and contribute to it when necessary. The goal is to persuade them to **shift their thinking** about security, from viewing it as some type of insurance or tax to valuing it as a business enabler.

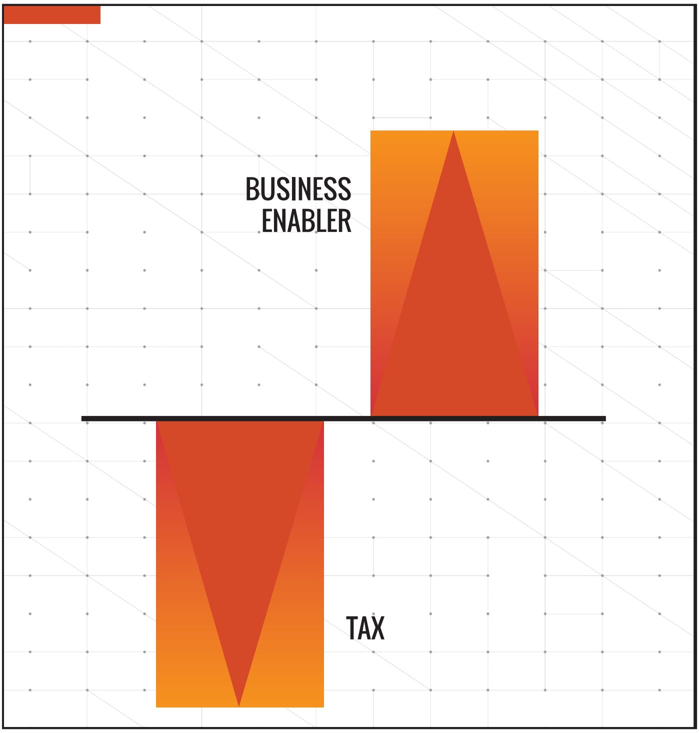


Figure 5-2: Shift thinking about cybersecurity from an insurance or tax to a business enabler.

To put skin in the game, they'll need to embrace cybersecurity for its ability to make a powerful and positive impact on the organization. Getting there involves illustrating just how critical security is to the mission and purpose of their particular function.

CAUTION

Robert Greene, author of *48 Laws of Power*, explains some of the considerations when shifting others' thinking: "In the realm of power you must learn to judge your moves by their long-term effects on other people. The problem in trying to prove a point or gain a victory through argument is that in the end you can never be certain how it affects the people you are arguing with: They may appear to agree with you politely, but inside they may resent you."[29]

[29] Robert Greene, *The 48 Laws of Power* (Viking Penguin, 1998), 72.

Make sure you have understanding, agreement, and commitment from your stakeholders—and underscore and renew these elements as often as necessary.

Influencing stakeholders as a leader

TIP

As the leader, you are responsible for shaping the mindsets of key stakeholders so they eventually behave in ways that support your goals. However, with such change comes an underlying–and often hidden–feeling of discomfort and anxiety about supporting you.

Greene states that "Human psychology contains many dualities, one of them being that even while people understand the need for change, knowing how important it is for institutions and individuals to be occasionally renewed, they are also irritated and upset by changes that affect them personally. They know that change is necessary and that novelty provides relief from boredom, but deep inside they cling to the past. Change in the abstract, or superficial change, they desire, but a change that upsets core habits and routines is deeply disturbing to them."[30]

Therefore, it is necessary to introduce change as organically as possible, with the least disruption to the business, your team members, and stakeholders.

You should frequently remind the organization why new processes are needed and the positive impact they can have or are having. Meet with stakeholders frequently to renew their support and see if there is a way to make that support public—it will give you more influence overall and a better chance of success.

[30] Ibid., 396-397.

Skills to develop

Establishing proper influence over key stakeholders is critically important. You simply won't be effective operating in your own bubble, so think about how you'll systematically do this on a continual basis. Consider the following practices:

- In educating your stakeholders, don't try to argue with someone's position. Instead, reveal to them cybersecurity dependencies that they never knew about. It's not always necessary to barge in with fear-mongering stories, but instead show them how cybersecurity is like the foundation to their home—a vital element that keeps it standing for the long term in the face of many adverse conditions.
- Remember that influence need not be overbearing (look to Servant Leadership in Chapter 4) or be externally bestowed; it can be earned through steady leadership, support that people value, or simply the emotionally intelligent way in which you carry yourself.
- As you implement changes for better security, talk through the possible impacts of those changes with stakeholders first to gain their opinions and guidance. Then collaborate with your team members to ensure you're choosing the best possible options to meet mutual goals.

3. Engage obstacles with perseverance

"Success is not final, failure is not fatal: It is the courage to continue that counts." – Winston Churchill

We have all faced adversity in our lives in one form or another. What successful leaders do differently is to analyze and directly address these challenges, and in the process, **transform obstacles into opportunities**. This is a skill that can be learned and shared with team members so that they can also persevere in the face of difficulty.

In fact, the authors of *Neuroscience for Leadership* claim, "Again and again we have found that it is not necessarily the brightest people with the highest IQ that have created the most value for their organizations and their societies, but those with persistence, resilience, tolerance of failure and risk and above all, self-management…"[31]

Ryan Holiday, author of *The Obstacle Is the Way*, explains how to accomplish this: "Overcoming obstacles is a discipline of three critical steps. It begins with how we look at our specific problems, our attitude or approach; then the energy and creativity with which we actively break them down and turn them into opportunities; finally, the cultivation and maintenance of an inner will that allows us to handle defeat and difficulty. It's three interdependent, interconnected, and fluidly contingent disciplines: *Perception, Action*, and the *Will*."[32]

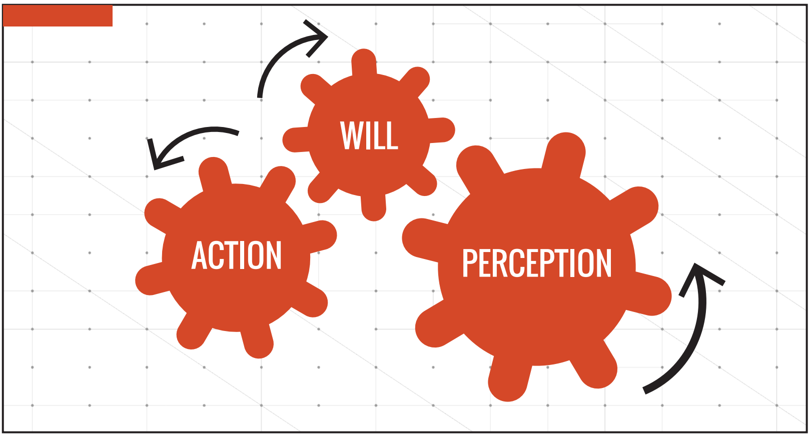


Figure 5-3: Engage obstacles with perseverance through perception, action, and will.

The first step is to think about an obstacle as an opportunity or an advantage, and then work resolutely towards solving it (which might mean working through it, around it, backing up from it, or changing the conditions for its original existence), and finally leaning on persistence to keep going.

Holiday says, "Placed in some situation that seems unchangeable and undeniably negative, we can turn it into a learning experience, a humbling experience, a chance to provide comfort to others."[33]

[31] Tara Swart, Kitty Chisholm, and Paul Brown, *Neuroscience for Leadership: Harnessing the Brain Gain Advantage*, 174.

[32] Ryan Holiday, *The Obstacle Is the Way* (Penguin Group, 2014), 9.

[33] Ibid., 125.

Working through cyber challenges

TIP

In the world of cybersecurity, we face challenges every day. The key here is not to give up, and to keep calm during calamities, no matter how difficult—even when there is unbearable pressure to perform during relentless attacks with untold consequences.

Or maybe you need to report to and satisfy five separate "bosses." Whatever the situation, we must accept this as the very essence of our work and lead with composure at all times.

Holiday elaborates, "To be great at something takes practice. Obstacles and adversity are no different. Though it would be easier to sit back and enjoy a cushy modern life, the upside of preparation is that we're not disposed to lose all of it—least of all our heads—when someone or something suddenly messes with our plans."[34]

Skills to develop

To turn obstacles into opportunities, you'll need to:

- Identify the current obstacles that you, your team members, and the organization face and, with your team, brainstorm the range of available options. Think through the cultural, political, financial, and technical variables at play—what's your best bet?
- Ask: how do these obstacles help us? How can we face them more effectively together?
- Practice level-headedness even if everyone else is panicking. Even when it seems like panicking is the natural thing to do. Breathe. Assess. Act. Repeat.
- Find comfort and encouragement knowing that–in conquering the obstacle–your program will become stronger and your team will become more confident on the other side.

Engaging obstacles with perseverance lays the groundwork for smart problem solving and sends a powerful message of self-control and "stick-to-it-ness" that positively influences teams and stakeholders. Let's look at another way to shape the environment for success.

[34] Ibid., 137.

4. Connect mind to mind

“The single biggest problem in communication is the illusion that it has taken place.” — George Bernard Shaw

Think of the most successful relationship you’ve ever had. Chances are, you developed a shared mental model that helped you and that other person think with one mind, creating synergy and ease around decisions and actions. This is known as **mental concordance**, and it’s just as important between leaders and their teams.

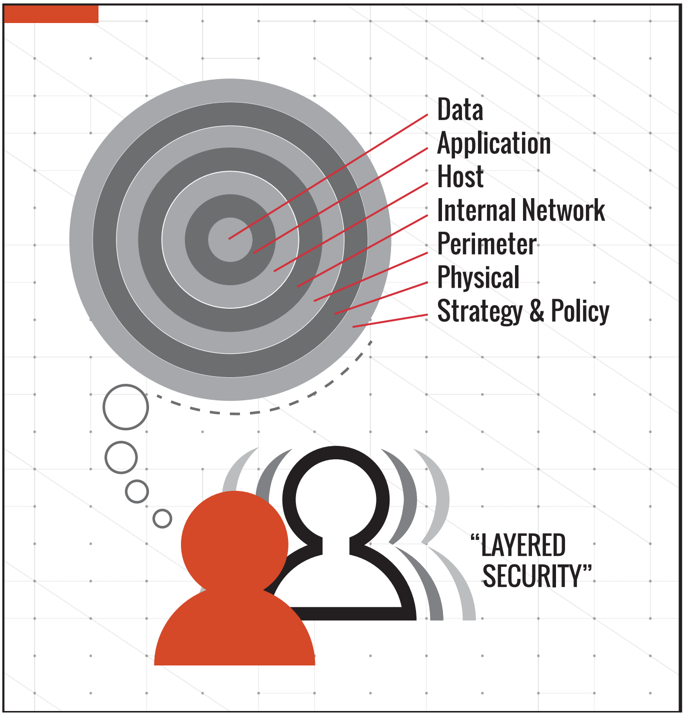


Figure 5-4: Develop a shared mental model that helps you and others think with one mind, creating synergy and ease around decisions and actions.

This is different from shared consciousness discussed in Chapter 4 in that we are speaking less about the logistics of integrating teams for better alignment and communication, and more about getting on the same wavelength within the team to shape on-the-ground decisions and behaviors.

The authors of *Neuroscience for Leadership* explain how it works: "When our brain is attempting to fill in meaning of another person's intent, from their words and/or actions, we are using an ability to interpret another person's mind.... This is a highly complex function without which operating effectively in a complex society would not be possible. Neuroscientists have begun to look at how this amazingly useful ability works. Some maintain that our ability to interpret another person's intent involves a specific part of the brain containing 'mirror neurons.' These fire in similar patterns as if to create the same movements, expressions and reactions that we are observing in another person."[35]

Because we are social beings, concordance is a skill we develop as we grow, and it is especially useful in leading teams. That's because, according to the authors, "Our brain needs a leader to create environments that feel safe and certain, even when the world is far from being either. We also need leaders who communicate well, who make understanding them easy, who create processes that are fair and transparent, so our brains do not waste precious effort in second-guessing them or trying to understand what to do next."[36]

The end result? "A good leader gets others around him or her to know, 'intuitively,' how he or she would assign weights to critical issues. In this way the mind of the leader usefully invades the minds of subordinates. The brain cells of subordinates do what the leader wants. That's culture. It's not just saying 'yes.' It is knowing what 'yes' would look like, feel like, be like."[37]

[35] Swart, Chisholm, and Brown, *Neuroscience for Leadership: Harnessing the Brain Gain Advantage,* 79.

[36] Ibid., 57.

[37] Ibid., 213.

Connecting the minds of the cybersecurity team

TIP

When a cyber incident strikes or an identified risk needs to be mitigated in a hurry, will you—as the leader—always be ready and available to make a key decision? Inevitably, the answer will be no. So, you need to trust your team—trust that they'll appreciate a situation in the same way you would, and act in accordance with your beliefs. Your task as a cyber leader is to develop this capacity in others at a scale that enables rapid and effective action in your business. That means you need to connect with them, mind to mind.

Establishing this mental concordance starts by realizing you are all parts of a greater whole, working for a greater good. And know that a quality relationship between a leader and a team acts as a social lubricant to ensure all parts are working together. To build trust with your team and establish a shared view of the world, you need to actively invest in developing and practicing the following skills.

Skills to develop

How well you develop mental concordance with your team is a determinant of how successful you and your program will be. Take this seriously. Establish trust and "one mind" with others so that you know everyone is moving in the same direction, with the same intent. Try the following:

- Understand that as the leader, your thoughts, behaviors, and actions resonate deeply with the people you lead. Think, communicate, and act in ways you want your team to emulate. Focus on the good–you want a positive culture.
- Develop a shared shorthand through embodied communications. For example, using a positive gesture that has a particular significance allows your team to understand your meaning immediately, even without words.
- Ensure you have fully explained your expectations to your team (and received confirmation of their understanding) about how to think through and act in critical situations.

Once you have connected mind-to-mind, you are in a position to create a high-performing culture. Let's look at that next.

5. Create a high-performing culture

"A leader is best when people barely know he exists, when his work is done, his aim fulfilled, they will say: we did it ourselves." – Lao Tzu

In days past, **creating a high-performing culture** might have consisted of fear-mongering and other negative manipulations. But as Daniel Pink's research highlighted in the last chapter points out, fear is not an effective motivator for performance. Other researchers agree. Swart, Chisholm, and Brown write, "Oddly enough most organizations still think mobilizing the escape/avoidance emotions will get results. After a fashion it does, but at a very high cost in terms of effort, money, and exhaustion. But nothing new or creative will happen that way. To achieve great organizational goals, management has to create the conditions under which individuals actively want to be doing what they are doing and stretch themselves far more. The basis of that is active trust, which only the leader can generate."[38]

According to Daniel Coyle, author of *The Culture Code: The Secrets of Highly Successful Groups*, a high-performing culture based on active trust is created by building safety—by ensuring belonging, sharing personal vulnerability, and establishing purpose to engage team members.

Coyle states, "Belonging cues are behaviors that create safe connection in groups. They include, among others, proximity, eye contact, energy, mimicry, turn taking, attention, body language, vocal pitch, consistency of emphasis, and whether everyone talks to everyone else in the group. Like any language, belonging cues can't be reduced to an isolated moment but rather consist of a steady pulse of interactions within a social relationship. Their function is to answer the ancient, ever-present questions glowing in our brains: *Are we safe here? What's our future with these people? Are there dangers lurking?*"[39] He goes on to underscore that "Group performance depends on behavior that communicates one powerful overarching idea: *We are safe and connected.*"[40]

[38] Ibid., 216.

[39] Daniel Coyle, *The Culture Code: The Secrets of Highly Successful Groups* (Bantam Books, 2018), 11.

[40] Ibid., 15.

Once the team feels safe and connected, cooperation can be enhanced by sharing deeper thoughts and feelings, which sends the message that this is a workplace where it's safe to express concerns and desires. Coyle states, "The mechanism of cooperation can be summed up as follows: *Exchanges of vulnerability, which we naturally tend to avoid, are the pathway through which trusting cooperation is built.*"[41]

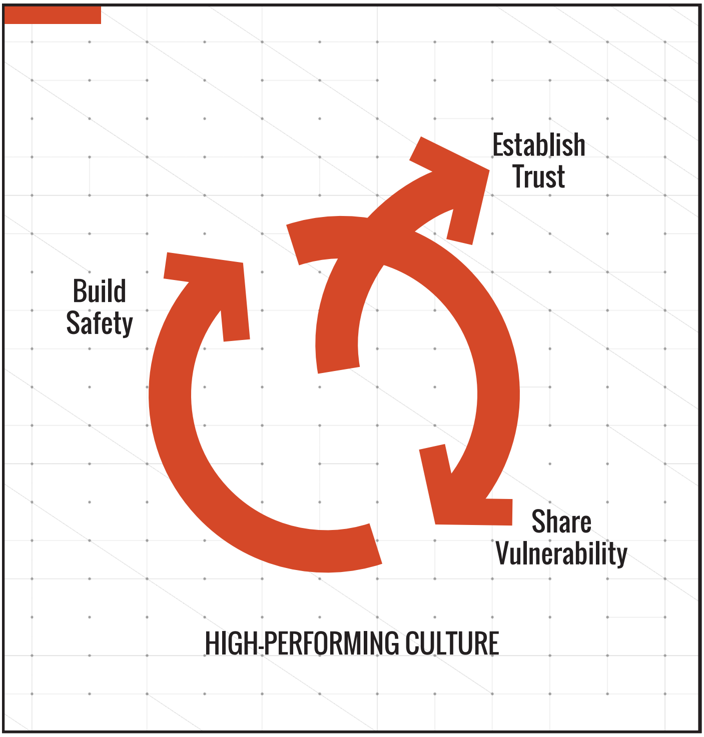


Figure 5-5: Elements of a high-performing culture.

[41] Ibid., 112.

This helps to bond team members so they can better work collaboratively towards a purpose. He continues, “High-purpose environments are filled with small, vivid signals designed to create a link between the present moment and a future ideal. They provide the two simple locators that every navigation process requires: *Here is where we are* and *Here is where we want to go*. The surprising thing, from a scientific point of view, is how responsive we are to this pattern of signaling.”[42] This is just one more way a cyber leader can shape an effective environment for success.

Creating a high-performing cybersecurity culture

TIP

Consider how you create belonging and trust within your team—and also how you don’t. When you think about it, you might realize you haven’t embraced everyone’s perspective and allowed them to commune within the group. Someone might have a very specific idea about what the biggest priorities are, and this view might be very different from yours or the rest of the team’s.

Be especially careful with those who do not agree with you to ensure you are not ostracizing them in some way. Everyone must feel like they belong, and everyone must trust each other, even in a high-pressure environment. In this way, your team members will be comfortable sharing their concerns and needs. Without these elements, you won’t have a high-functioning team.

Lastly, make sure, as we discussed in Chapter 4, that you have aligned everyone behind a mutual goal that is meaningful and significant to create a purpose towards which people are willing to work together.

[42] Ibid., 180.

Skills to develop

As the cyber leader, realize that you're responsible for cultivating a cultural microcosm within your organization. This is your program and your team. You're not compelled to adopt and simply live with the broader company culture. Make it what it needs to be by practicing the following:

- Look for opportunities to build assurances of safety within the team by responding positively to negative feedback or bad news, by taking responsibility for someone's mistakes (you're the leader; it's your job), or by encouraging candid discussion without repercussions.
- Once you've built trust and belonging, think about how you can get the group to open up and share personal vulnerabilities. Many organizations leap to formal group exercises and survival courses, but this isn't really necessary—there are plenty of opportunities to share concerns and desires in any modern workplace.
- Ensure everyone knows why their work is important, the impact that it has, and how it supports the larger goals of the department and organization.

In the next chapter, "Principle 3: Orchestrate," we'll look at how you can structure and choreograph resources to serve agilely and optimally.

Chapter 6

Principle 3: Orchestrate

In this chapter

- Create a nimble and effective team and program
- Lead in a way that naturally elevates your team members' performance
- Understand ways to create trust and collaboration with external teams
- Adapt to fast-changing business models, technology architectures, and cyber risk environments

"If you want something new, you have to stop doing something old."

– Peter Drucker

In the previous chapter, we learned how to shape not only the values, expectations, and behavior of your teams, but also those of the broader enterprise. Now that those elements are in place, you are in a position to **orchestrate**, by which I mean to structure and choreograph resources to deliver security in the most agile and optimal way possible.

As the leader, you are the **security program's maestro**—conjuring up an artistic experience that your team members and stakeholders will remember and think highly of. It's your job to get the very best out of the people, processes, and tools at your disposal, even in tumultuous times. Sometimes you'll be hands on; at other times you'll empower others to execute. Regardless, the maestro ensures the orchestra is in harmony and that the audience gets their money's worth.

The Need to Orchestrate

As we've seen in previous chapters, you as the leader must illuminate the path you want your team to take, starting with yourself and then directly influencing your team members and the culture. Ray Dalio, author of *Principles*, underscores this: "Of course, the higher up you are in an organization, the more important vision and creativity become, but you still must have the skills required to manage/orchestrate well."[43] Let's look at how to bring it all together and marshal resources to make it happen.

As we've noted before, there are four key sub-principles that enable you to orchestrate as a leader:

DON'T FORGET

1. **Train for Agility—**Ensuring nimbleness is baked into the DNA of your security program.
2. **Stir Excitement about New Skills—**Creating an environment that raises the bar to get the very best from your people.
3. **Multiply Forces with a "Team of Teams" Approach—**Developing a relational web across teams to stimulate trust and collaboration.
4. **Embrace Change When Needed—**Learning to adapt to evolving conditions.

Let's take a closer look.

1. Train for agility

"Success today requires the agility and drive to constantly rethink, reinvigorate, react, and reinvent."
– Bill Gates

The cybersecurity world is changing fast, and one of the best ways we can keep up is by becoming agile in our attitudes and responses to change. This notion is best expressed by Pamela Meyer, author of *The Agility Shift: Creating Agile and Effective Leaders, Teams, and Organizations*. She says, "The Agility Shift is the intentional development of the competence, capacity, and confidence to learn, adapt, and innovate in

[43] Dalio, *Principles*, 451.

changing contexts for sustainable success."[44] In other words, **training for agility**.

She advises that "organizations making the agility shift need to think beyond competence-based learning and create conditions and opportunities for all of their players to perform at their best. This does not mean overlooking competence; it means thinking of competence as the pathway to performance, when competence meets confidence and capacity in action."[45] Thus, agility means not only being able to respond appropriately, but doing so fearlessly and putting the right plans in motion.

Key to becoming more agile is the ability to create "relational webs," which Meyer describes as personal and organizational networks for support, coordination, and sharing of both ideas and resources. She says our relational webs help us make sense of what is happening and determine its significance, creating the conditions to respond in a more agile manner.

Beyond that, "The most effective and agile leaders, teams, and organizations do more than weave a strong Relational Web. They adopt a mindset, strategy, and practices that ensure they are relevant, responsive, resilient, resourceful, and reflective."[46] In Chapter 4 we saw the importance of a growth mindset—a critically important organizational characteristic that enables a shift to agile operations.

Creating agility in your cyber organization

TIP

There's so much that changes in cybersecurity. Think about when the business establishes a new product-service mix, when new suppliers are added, when the old technology infrastructure is uprooted and replaced, or simply when a new threat variant hits the wild. All of this is hugely relevant—and disruptive—to the "how" and "what" of implementing cybersecurity in your enterprise.

While high dexterity in cyber incident response is a piece of the puzzle, leaders must look at agility through a much

[44] Pamela Meyer, *The Agility Shift: Creating Agile and Effective Leaders, Teams, and Organizations* (Bibliomotion, 2015), 3.

[45] Ibid., 132.

[46] Ibid., 25.

broader lens. As outlined above, the macro changes in a business can have huge ramifications for your security program. So, as you truly begin to embrace the strategic importance of agility, you can begin creating strong relational webs. At the core, that means designing for people, not machines.

Meyer explains, "The knowledge that agile organizations are more profitable, sustainable, and innovative may be reason enough for you and your organization to make the agility shift. However, this shift is not only practical—ensuring your ability to survive and thrive—its core dynamics (interacting and interconnecting) are the key to your ability to create and experience meaningful purpose, and happiness....essential to fostering and sustaining the level of engagement, commitment, and creativity you need to respond effectively when the unexpected hits."[47] That means ensuring that you and your team members have plenty of opportunities to connect with each other and other members across the enterprise.

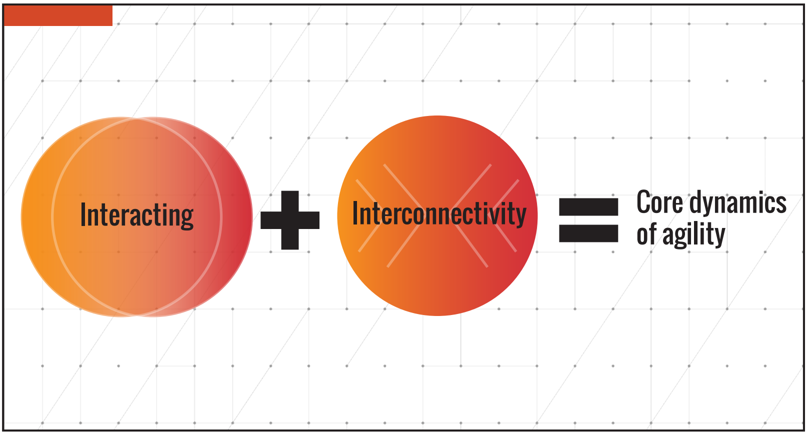


Figure 6-1: Agility is key to your ability to create and experience meaningful purpose.

[47] Ibid., 7-8.

I realize that "agile" is thrown around quite loosely these days, and that it may fall on deaf ears due to overuse. But take this concept seriously. Think hard about why you might need to make your entire cyber program more nimble, and design appropriate features into your capability portfolio and operating model that make it real.

Skills to develop

Think through the processes you need to create an agile program (we're talking more broadly than DevOps here). It starts with people and recruiting for the right qualities—and then recognizing and reinforcing those qualities to retain the best performers. It's also about organizational design and operational processes. Think about:

- The processes you can install to help your people build relationships that will help them think on their feet and make the best decisions.
- How to foster cross-functional collaboration and a healthy degree of interdependence.
- The specific capabilities you might need to ensure organizational agility (e.g., business leader engagement, supply chain risk analytics).
- The elements and structures you need to help your team members become resilient and responsive.
- What you can do to attract and keep open-minded team members.
- How to reward agility and adaptation to changing circumstances.
- Exercises (e.g., wargames, tabletops) to stress-test and improve organizational agility.

We've reflected on the importance of training for agility. Let's now look at how to engage the team to learn new skills and make great use of that agility.

2. Stir excitement about new skills

"Before you are a leader, success is all about growing yourself. When you become a leader, success is all about growing others." – Jack Welch

One of the best ways to generate excitement about skill acquisition is to create an environment in which everyone wants to learn, contribute, and grow. Liz Wiseman, author of *Multipliers: How the Best Leaders Make Everyone Smart,* explains: "With the explosion of information...there is simply too much for any one person to know. Consequently, the role of the leader has shifted, too—moving away from a model where the manager knows, directs, and tells and toward one where the leader sees, provokes, asks, and unleashes the capabilities of others."[48] Wiseman categorizes leaders as either **multipliers** who expand the skills of the people around them, or diminishers who squash talent and engagement.

From observing multiplier leadership at a former employer, Wiseman concludes, "Multipliers are genius makers. What we mean by that is that they make everyone around them smarter and more capable. Multipliers invoke each person's unique intelligence and create an atmosphere of genius—innovation, productive effort, and collective intelligence."[49]

How do you know if you are a multiplier? Wiseman suggests, "Multipliers look at the complex opportunities and challenges swirling around them and think, *There are smart people everywhere who will figure this out and get even smarter in the process*. And they see that their job is to bring the right people together in an environment that liberates everyone's best thinking—and then to get out of their way and let them do it."[50]

[48] Liz Wiseman, *Multipliers: How the Best Leaders Make Everyone Smarter* (HarperCollins, 2017), xvii.
[49] Ibid., 5.
[50] Ibid., 18.

Becoming a multiplier of cyber-relevant skill and talent

TIP

Reading about multipliers, you might think that it's all about giving positive feedback to help your team thrive. That's actually not the case. Interestingly, Wiseman says, "One of our most critical insights from our study of Multipliers is how hard-edged these managers are. They expect great things from their people and drive them to achieve extraordinary results. They are beyond results-driven; they are tough and exacting. Indeed, Multipliers make people feel smart and capable, but they don't do it by being 'feel good' managers. They look into people and find capability, and they want to access all of it and utilize people to their fullest. They see a lot, so they expect a lot."[51]

As a cyber leader, you need to look for those budding flowers—those **hints of skill and passion that are burgeoning within people, just waiting to be unleashed**. These skills might fit their current roles, or they might not. But you must be scanning for these high-value attributes, such as entrepreneurial spirit, technical architecture design skills, interpersonal communication or marketing ability, or an understanding of vision setting. It's undeniable that successful cyber programs today require a very diverse mix of skills. Many of them are atypical. As the cyber leader, it's your job to understand, scan for, and promote these skills in people.

[51] Ibid., 24.

Skills to develop

According to Wiseman, there are five disciplines of a multiplier[51]:

1) Attracting and optimizing talent
2) Creating intensity that requires best thinking
3) Extending challenges
4) Debating decisions
5) Instilling ownership and accountability

She recommends, "Instead of trying to develop strength in all five disciplines, an aspiring Multiplier should set an extreme development plan. Begin by assessing your leadership practices and then work the two extremes: 1) neutralize a weakness 2) top off a strength."[52]

Furthermore, cyber leaders can ask themselves the following questions:

- Do I understand the true mix of technical and non-technical skills needed for our program to succeed?
- Have I identified who does or might possess those skills?
- How will I gain access to skills that are current gaps for us?
- What can we do to encourage new skill acquisition?

Next, let's look at how to build on this sub-principle by applying these skills in conjunction with other teams.

3. Multiply forces with a "Team of Teams" approach

"None of us is as smart as all of us." – Ken Blanchard

We discussed the **Team of Teams** approach in Chapter 4 and it bears deeper examination to see how it applies to the principle of orchestration. According to General Stanley McChrystal, author of *Team of Teams: New Rules of Engagement for a Complex World*, "On a single team, every individual needs to know every other individual in order to build trust, and they need to maintain comprehensive awareness at all times in order to maintain common purpose—easy with a group of twenty-five, doable with a group of fifty, tricky above one hundred, and definitely impossible across a task force of seven thousand. But on

[52] Ibid., 21-22.
[53] Ibid., 251.

a team of teams, every individual does not have to have a relationship with every other individual; instead, the relationships between the constituent teams need to resemble those between individuals on a given team…"[54] In this way, your team becomes interconnected with other teams and not separated, which helps with information sharing, decision making, organizational agility, and, ultimately, better results.

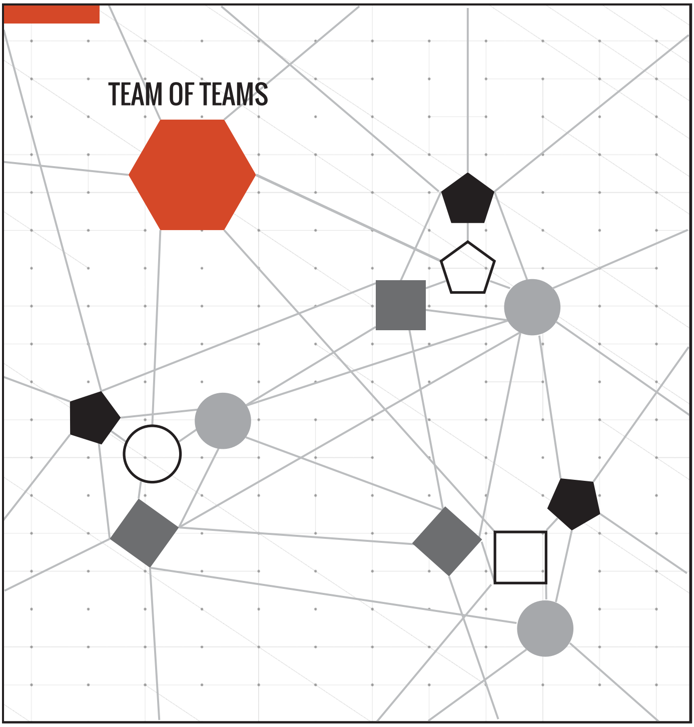


Figure 6-2: Relationships between constituent teams need to resemble those between individuals on a given team.

[54] McChrystal, *Team of Teams: New Rules of Engagement for a Complex World*, 128.

Expanding reach and trust to maximize cybersecurity impact

TIP

A team is greater than the sum of its parts if they have developed trust and collaboration not only with each other but also with other teams within (and outside of) the enterprise. As a cyber leader, your job is to break down silos and help members of your team build relationships with members of other teams. This recommendation is much like Meyer's idea of building relational webs to foster organizational agility. And it starts with you: make sure you have built your own relational web before ensuring others do so as well. Model to your team the value and approach of becoming networked outside of your own comfort zone.

Especially in large organizations, cybersecurity programs cannot be successful by living in a box. The people within these teams need to identify and nurture partners who embrace and contribute to the mission. There are simply too many challenges that exist outside of a security program's natural span of control. You need assistance. And that's just the reality.

Skills to develop

If you're working in a large organization, a Team of Teams approach will be critical to success. Learn to build bridges with other internal (and external) organizations—particularly those that hold the most sway and/or can most directly deliver tangible support to securing the business. For example:

- Build a tight alliance with the Chief Technology Officer (CTO) organization to ensure you're in mutual alignment regarding how infrastructure decisions and security need to be in lockstep.
- Develop a shared philosophy with the Enterprise Risk Management group on how cyber risk information can be most effectively elevated to the highest levels of the business for decision making.
- Provide technical support to the R&D business unit to ensure they're proactively planning for and implementing "secure-by-design" principles when developing new products and services.
- Work with corporate communications and marketing to determine if cybersecurity can/should be woven into the company's externally facing value proposition. See if there are specific events where you or your team members could have a speaking role.

Lastly, after we've built agility, nurtured a skill acquisition culture, and created a force multiplier effect with the broader enterprise, we must still recognize that change is a constant in the cyber world. Here's how to deal with it and help your team do so as well.

4. Embrace change when needed

"It is not the strongest or the most intelligent who will survive but those who can best manage change."
— Charles Darwin

Even when change is not difficult, it can be disruptive and unsettling if we are not prepared for it. Of course, if you have trained for agility, it will be easier. Still, Ray Dalio, author of *Principles*, suggests: "Recognize that change is difficult. Anything that requires change can be difficult. Yet in order to learn and grow and make progress, you must change. When facing a change, ask yourself: Am I being open-minded? Or am I being resistant? Confront your difficulties head-on, force yourself to explore where they come from, and you'll find that you'll learn a lot."[55]

Dalio describes a process to help ensure you **navigate change** successfully. The steps include having a clear goal, identifying and eliminating problems that stand in the way of your goals, diagnosing problems to understand their root cause, designing plans to get around problems, and doing what's necessary to complete these plans. It sounds fairly straightforward, but to deal with the transition, he offers this suggestion: "Recognize that design is an iterative process. Between a bad 'now' and a good 'then' is a 'working through it' period. That 'working through it' period is when you try out different processes and people, seeing what goes well or poorly, learning from the iterations, and moving toward the ideal systematic design. Even with a good future design picture in mind, it will naturally take some mistakes and learning to get to a good 'then' state."[56]

You should help others embrace change. Dalio notes: "Don't confuse the quality of someone's circumstances with the quality of their approach to dealing with the circumstances. One can be good and the other can be bad, and it's easy to confuse which is which. Such confusion is especially common in organizations that are doing new things and evolving fast but have yet gotten the kinks out."[57] You must look beyond **what** your people are dealing with and instead assess **how** they are dealing with it.

Persevering in the face of cybersecurity change

TIP

Unfortunately, much of the change that happens in the cyber world is linked to negative events, and we must learn to deal with the inevitable adversity that we will face (and cannot truly plan for). That is simply the nature of our world. I'm thinking of recent cyber incidents such as NotPetya that can completely derail daily operations. As much as you have trained for agility and planned for change, it's unlikely you've thought of everything.

[55] Dalio, *Principles*, 434.

[56] Ibid., 501-502.

[57] Ibid., 489.

Perhaps you are suddenly wrestling with a large-scale organizational redesign that severely affects the program's once-strong organizational positioning and authority foothold. What will you do? How will you respond? And how will you set the example for your team to process these unsettling changes?

One way to successfully embrace change is to have a system in place to manage it, such as the "Observe, Orient, Decide, and Act" (OODA) loop, developed by military strategist John Boyd as a means of succeeding in uncertain times.[58] Change will happen repeatedly, so get systematic about it. The cyber world is uncertain (at the best of times), and you will need processes and collective ingenuity to stare down and persevere through these changes.

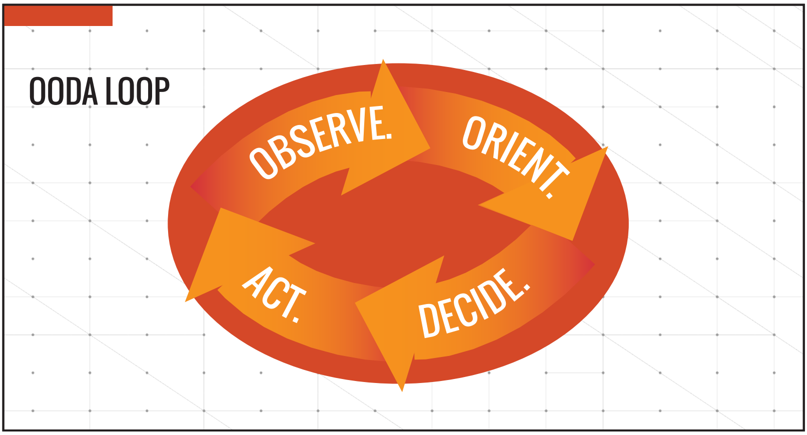


Figure 6-3: The four steps of the OODA Loop.

Dalio provides this change analogy: "Understand the power of the 'cleansing storm.' In nature, cleansing storms are big, infrequent events that clear out all the overgrowth that's accumulated during good times. Forests need these storms to be healthy—without them, there would be more weak trees and a buildup of overgrowth that stifles other growth. The same is true for companies. Bad times that force cutbacks so only the strongest and most essential employees (or companies)

[58] Richard Feloni and Anaele Pelisson, "A retired Marine and elite fighter pilot breaks down the OODA Loop," BusinessInsider.com, August 13, 2017. http://www.businessinsider.com/ooda-loop-decision-making-2017-8

survive are inevitable and can be great, even though they seem terrible at the time."[59] Have you or your program undergone a cleansing storm lately? If not, it might be long overdue—anticipate that one is already on the horizon and headed your way. What will you do to prepare?

Skills to develop

Much of this chapter has been devoted to developing resilience, agility, and interconnectedness to weather the vast changes we face every day. Here's what you can do to lead more effectively in changing times:

- Assume everything can change in an instant and plan for it. What is the worst that can happen? Think bigger than a cyber incident. What if your program's budget is cut severely? What if a new leadership regime no longer politically supports you? Make a plan for how to deal with it.
- Ensure your professional relationships are respectful, supportive, and strong—you'll need those connections to weather changes. Continually check in with these people to nurture this rapport.
- See to it that your team members anticipate and embrace change. Set an expectation that nothing stays the same and that no one should expect it to. With this mindset, it'll be far less jarring to their world when the change occurs.

In the next chapter, "Bringing the Concept to Life," we'll look at advice and guidance on how to move forward with all of the principles of cyber leadership.

[59] Dalio, *Principles*, 502.

Chapter 7

Bringing the Concept to Life

In this chapter

- Delve into two examples of the principles in practice
- Reflect on substantive barriers that impede progress
- Look at how cyber leaders unlock real change in their worlds
- See specific steps taken to catalyze, shape, and orchestrate teams and organizations

We've laid the foundation for modern cyber leadership with four key principles and 16 sub-principles. Let's now look at how they apply in the real world. We'll review two specific cases where these principles made a significant difference in the mindset and behavior of cyber leaders and their teams, resulting in enhanced security appreciation and activities in the overall organization. As you read through these examples, think about how they might apply to your organization's unique challenges and cultural dynamics.

Case Study #1: Global 100 Industrial Conglomerate

Our first case is a global company with a large-scale manufacturing footprint in the majority of countries, necessitating a large, complex IT infrastructure. Further complicating things is the fact that more than half of the company's product portfolio is Internet-connected.

Challenges

Like many distributed businesses grown through acquisition, this enterprise grappled with three distinct cybersecurity issues:

1. Understanding of and support for cybersecurity was highly variable across business units and geographies.
2. Given the complex organizational structure, the security team lacked strong positioning to exert proper influence.
3. The infrastructure was designed for business efficiency, not security.

Let's look at each of these challenges:

1) Unsupportive Organizational Culture

In this global organization, revenue-producing business units held the power. Culturally, everyone else took a back seat. And because most business leaders saw cybersecurity as a "purely IT issue," they deemed it non-essential to operations. It was perceived as simply a back-office tax. This mindset resulted in minimal top-down leadership initiatives or messaging that promoted security as essential to the business.

2) Non-Influential Security Organization

Compounding this challenge was the fact that power dynamics were influenced and largely determined by how "close" you were to company headquarters, both literally and figuratively. This didn't bode well for the security program, which was buried two layers down under the global CIO (and geographically separated).

These circumstances were worsened by the security program's need to employ a federated structure of business information security officers (BISOs) supporting major global regions. Because these locations were often far-away from headquarters, the BISOs lacked real influence over their localities.

3) Efficiency Prioritized over Security

Lastly, for cost savings, the enterprise maintained a flat network architecture that inherently made it hard to secure specific parts of the business. And because the company also lacked a clear view of its critical business assets (e.g., systems, business processes, etc.), it was hard to prioritize security efforts. In this way, the infrastructure was designed more for efficiency than security.

Tackling the challenges with leadership

Realizing that these challenges were holding the cyber team back and hampering security efforts, the global CISO (the organization's principal cyber leader) looked for a methodical approach to improvement.

She realized the cyber talent base was strong enough to build upon, but the business environment in which the security program was operating was not well suited to accept or even appreciate what the program could deliver.

She decided to undertake a massive **"Shape"** (Principle 2) and **"Orchestrate"** (Principle 3) initiative. As it would take some time, a two-pronged approach—influencing corporate business leadership and regional business leadership at the same time—was needed.

The CISO began by establishing an aligning narrative and then systematically conducting organizational change management activities to shift how the corporate and regional leadership teams perceived security—from a tax to an enabler. Here's how she jumpstarted the effort.

Implementing the "Shape" Principle

The CISO began with the sub-principle **"Embrace the Perspectives of Others"** by forming a transformation management office to systematically prepare for the long road ahead. Initially, this office held internal brainstorming meetings to gauge the likely perspectives of the various stakeholder communities that were important to the security program's success. First, they reviewed each group's power (degree of influence) and interests (what they cared about).

This gave them data they could test, and the team then used a few trusted internal parties to validate these hypotheses.

After developing a viewpoint on what each stakeholder group cared about, the CISO and team set about implementing the sub-principle, **"Influence Your Stakeholders' Mindsets and Priorities."**

They conducted a roadshow to meet with these business leaders, carefully empathizing with their concerns and needs while intelligently pressing the security agenda. Because the team had prepared carefully, security vs. business friction was reduced, and the business stakeholders appreciated the security team's efforts to understand and fine-tune their approach to account for business needs. This resulted in a positive, "meet-in-the-middle" approach that began to establish long-term trust and transparency.

As the last step in shaping, the team worked to **"Engage Obstacles with Perseverance."** Inevitably, their efforts ran into challenges, particularly as the security teams worked the next layers down on both the business and IT sides. The second and third layers of business units naturally had their own priorities, even "shadow security" efforts such as custom endpoint monitoring that differed from corporate guidance. Overcoming these issues required finding a local champion to advocate on the CISO's behalf; this "insider" approach helped smooth over extended confrontation and resistance.

Orchestrating for Success

During the year the CISO worked on changing stakeholder viewpoints. In parallel, she tasked her deputy to focus on careful orchestration of a hybrid security program operating model: a combination of corporate-led shared services paired with region-led localized security programs (where specific tailoring could take place).

The first sub-principle they implemented was to **"Train for Agility."** During their shaping efforts, the security organization had worked diligently to prepare for increased responsibility and visibility. By vying for more influence in the business, they needed to ensure they were a top-performing organization. So, during that time, they went through a concentrated range of stress test exercises and improvement efforts (such as tabletops, wargames, and red teams) to identify gaps and determine how they could be more nimble.

These efforts evolved the program to the point where a new "launch" could be marketed, following preparation of the business to receive this message.

After a year of very difficult but productive shaping activities, the CISO organization (and federated regional programs) began new projects that went beyond “business-as-usual” efforts. At this point, the team was well trained and exercised, and ready to perform.

In year two, the CISO started to **“Multiply Forces with a ‘Team of Teams’ Approach.”** Because the business was so complex and sprawling, the security program couldn’t go it alone; there were simply too many dependencies in working with other teams—IT infrastructure, product and service development, and manufacturing, just to name a few.

Using this approach meant connecting the core security team with important alliance teams across the business. This was an important evolution in the operating model to ensure continued buy-in and durability of the program in the face of inevitable company transformation (e.g., leadership and structural changes).

Gauging success and looking forward

This CISO-led initiative resulted in massive structural changes in security program operations. Therefore, the typical metrics for gauging security progress only told a piece of the story (e.g., vulnerability management coverage, time to detect, etc.). To accurately measure results, the CISO added innovative return on investment (ROI) metrics. For example:

- ☑ Whether security had a regular seat at technology strategy steering committee meetings
- ☑ How much of the security workload was being taken on and actually funded by the business
- ☑ Degree of extra focus on critical business assets

In addition, the organization instituted “cyber risk” as a separate risk type within the Enterprise Risk Management program, acknowledging its supreme relevance to business health for the first time.

Case Study #2: Global 50 Automaker

Our second case study focuses on a global 50 automaker with numerous brands worldwide. This organization offers a highly tailored product, service, and business model mix based on geography.

Challenges

Like our last case, this organization suffered from three main challenges:

- ☑ An engineering-first mentality limited security's contribution to the business.
- ☑ There was a dominant focus on business technology evolution, without security as a main feature.
- ☑ The company lacked a centralized security function, creating additional gaps and risk.

Let's take a closer look.

1) Engineering-First Mentality

As with many manufacturers, this organization perceived any business unit not obviously contributing to product development (through R&D or manufacturing) as "second tier"—and unfortunately, cybersecurity was one of them.

The general mindset was simply that every problem was fixable through engineering; physics was the only relevant battle. This meant that anything related to IT needed to be about cost-cutting, since IT wasn't directly contributing to vehicle development, production, and market share.

2) Technology Advancements without Security

While trying to make big leaps forward in technology, the company neglected the security implications. For example, the organization was exploring many new capabilities in cloud, analytics, smart manufacturing, and connected products, but did not acknowledge (and therefore did not address) that these projects inherently created large-scale security risk.

3) Vertical Security Ownership

The previous issue was made worse by the fact that security was "owned" by multiple verticals, with differing levels of authority, As a result, security was handled very differently and independently by the IT, product, and OT (manufacturing) organizations.

Unfortunately, there were many interdependencies between these organizations; security issues cannot be contained within siloes. This meant that the biggest problems were at the organizational seams, where risks mounted. No one person or group was well-positioned to solve this pervasive problem, leaving things to fall through the cracks.

Leaders step in

After a series of cyber incidents in multiple verticals, top company leaders realized that having various security factions created more problems than it solved. Fortunately, one of these leaders in charge of product cybersecurity had a strong understanding of the interdependent issues. His position in the product development community gave him greater access to and influence over some powerful leaders within the broader enterprise. Company executives asked him to unify efforts.

In considering the greater health of the business, this cyber leader worked to combine disparate security silos under a single construct, with IT, OT, and product organizations working together rather than independent of each other.

Self-Reflection Builds the Foundation

Through self-reflection, this leader realized he could **"Embody a Growth Mindset."** This was an extremely tough environment to be effective in cybersecurity—many had tried and ultimately failed. But what worked in his favor was for a history of advancing in the organization by taking on newly established roles that required him to learn in a hurry (some roles were even outside cybersecurity).

He had built a unique worldview with a growth mindset—valuing new experiences and learning, and appreciating the perspectives of others.

Second, he understood the importance of this sub-principle: **"Open Yourself to Feedback."** Once in the product cybersecurity space, he took on many battles on behalf of his organization. His job was to infuse cybersecurity requirements and tradecraft into the vehicle design process.

This mission required him to serve as the "punching bag" for his team as they slowly made progress. Even though he received a lot of feedback over time—some of it quite harsh—he knew it would ultimately help the organization. And it did.

He also was a leader who could **"Serve to Empower Others,"** one of the most important sub-principles he practiced. He always valued growing his team and concentrated on coaching his direct reports, giving them many opportunities to drive initiatives on their own and learn in the process.

Essentially, he invested in his high-potential team members, as they'd be succeeding him one day. Over time, his team evolved into a highly tuned machine for product cybersecurity. So when senior executives saw the glaring need for a broader cyber change, his team was well positioned to carry on the product cyber mission.

Catalyzing Teams with a Company-Wide Vision

In implementing the "Catalyze" principle, he first endeavored to **"Express a Driving Purpose."** In a massive, multinational company with many competing agendas, getting broad-scale support for anything is a daunting effort. However, because the company had experienced a range of cyber incidents in multiple domains, the top-level leaders (including the CEO) realized something had to change; these gaps in coverage across environments couldn't continue.

Because the product cyber lead had already made significant headway in a tough environment, when he was called upon to build a company-wide cybersecurity program that integrated IT, OT, and product, he was able to establish a strong vision for success. This vision united previously divided factions under a common rationale with an alignment on strategy that had previously been absent.

To help carry this out, he sought to **"Proliferate a Shared Consciousness."** This took serious effort, as company politics made the environment extremely divisive. Having a message is one thing, but unifying diverse groups to the point where they all truly believe in that message is quite another. It took a "Team of Teams" approach to minimize political drama. The cyber leader established champions across previously separate groups and asked them to sponsor the message locally.

In doing so, he had to **"Simplify the Complexity and Noise."** The company itself was innately complex, and arriving at a streamlined cybersecurity message was no cakewalk. With all the upheaval in establishing a unified security organization, combined with remaining skepticism about cybersecurity, there was quite a bit of noise to weed out. He relied on marketing professionals around him to ready the message.

In such a hard-to-grasp, constantly changing environment, there was no room for ambiguity in what they were trying to do. Simplicity of message was key and so the leader streamlined the program's vision to its essence, distilling the program's vision down to a series of operating principles and strategic objectives.

The groundwork is developed

These efforts laid the groundwork for program build-out and cleared the path for executing Principles 2 and 3 in the future. For now, this organization is benefiting from cross-domain exercises and strategic planning for the first time, helping to create alignment across divisions and minimize functional and political siloes.

To support these efforts, they've undertaken consolidated security policy development—tailoring shared policy at the top level for other domains at lower levels. To make sure these activities are effective, the organization instituted a range of qualitative and quantitative metrics to gauge adoption of desired practices and behaviors—driving accountability as well as results.

Resources

More information about the authors featured in this book can be found here:

Lisa Bodell: futurethink.com

Paul Brown: thefearfreeorganization.com

Kitty Chisholm: boardwalkleadership.com

Daniel Coyle: danielcoyle.com

Ray Dalio: principles.com

Carol Dweck: mindsetonline.com

Adam Grant: giveandtake.com

Robert Greene: powerseductionandwar.com

Robert Greenleaf: greenleaf.org

Ryan Holiday: ryanholiday.net

General Stanley McChrystal: mcchrystalgroup.com/insights/teamofteams/

Pamela Meyer: pamela-meyer.com

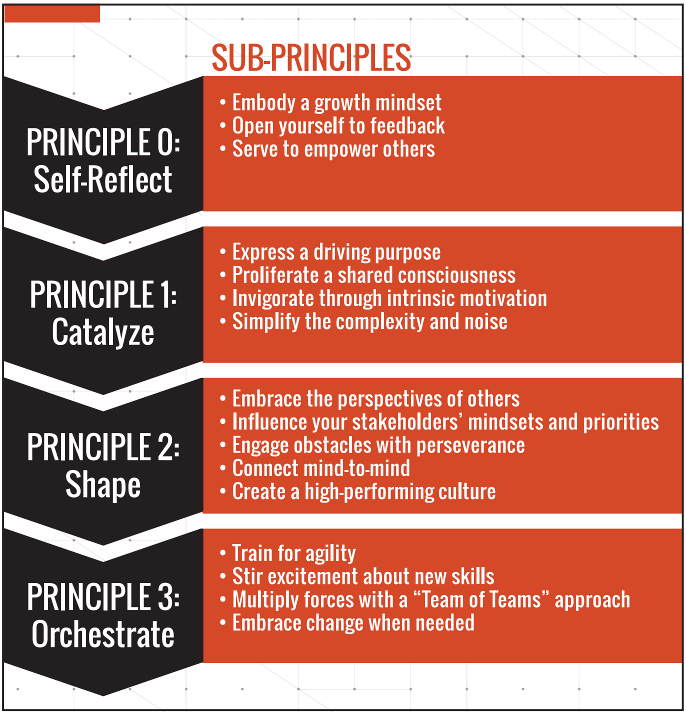
Daniel Pink: danpink.com

Simon Sinek: startwithwhy.com

Tara Swart: the-unlimited-mind.com

Liz Wiseman: multipliersbooks.com

Appendix



SUB-PRINCIPLES

PRINCIPLE 0: Self-Reflect

- Embody a growth mindset
- Open yourself to feedback
- Serve to empower others

PRINCIPLE 1: Catalyze

- Express a driving purpose
- Proliferate a shared consciousness
- Invigorate through intrinsic motivation
- Simplify the complexity and noise

PRINCIPLE 2: Shape

- Embrace the perspectives of others
- Influence your stakeholders' mindsets and priorities
- Engage obstacles with perseverance
- Connect mind-to-mind
- Create a high-performing culture

PRINCIPLE 3: Orchestrate

- Train for agility
- Stir excitement about new skills
- Multiply forces with a "Team of Teams" approach
- Embrace change when needed

Figure A: Four key principles and their sub-principles for effective cyber leadership.

Glossary

autonomy: The desire and ability to direct our own lives.

catalyze (Principle 1): Cultivating a vision and a following by employing psychology to grow, inspire, and align teams.

"down and in": Focusing communications and activities toward team members within your direct span of control.

driving purpose: An aligning narrative that describes why your organization does what it does, its values and principles, and what the results should be.

embodied communication: Gestures, facial expressions, and body language that convey meaning.

empathy: Putting yourself in the shoes of other people to embrace their perspective and better understand what motivates their behavior.

growth mindset: The belief that new abilities can and should be continually developed.

intrinsic motivation: Understanding what makes your key audiences tick and using that psychology to inspire them.

mastery: The intrinsic need to improve at something that matters to us.

mental concordance: A shared mental model that helps you and others think and act with one mind.

multiplier: A person who expands the skills of those around them by invoking each individual's unique intelligence.

OODA (Observe, Orient, Decide, and Act) loop: A decision framework to help people succeed in uncertain times.

operational technology (OT): Hardware and software that monitors and/or controls physical devices to detect or cause changes.

orchestrate (Principle 3): Structuring and choreographing resources to serve the business as agilely and optimally as possible.

organizational agility: The ability to respond nimbly as a team, as a program, and as an enterprise.

purpose: The yearning to work in the service of something larger than ourselves.

radical transparency: Examining one's ideas with others and being open to and accepting of feedback.

self-reflect (Principle 0): Looking inward to better know ourselves. Self-reflection helps us interpret how our actions affect the lives of others.

servant leadership: Using a leadership position to help others become their best selves. The idea is to serve your team members by meeting their needs, expectations, and values before leading them.

shape (Principle 2): Molding your internal and external environments to win hearts and minds and improve your odds of success.

shared consciousness: Creating a shared worldview whose vision, mission, and purpose are known and embraced by everyone.

team of teams: A relational web across teams that creates trust and promotes collaboration.

"up and out": Communicating with and influencing the broader stakeholder community to enable your program's success.

vision: The greater, long-range purpose towards which you and your team are working.

Explore four timeless principles for successful cyber leadership. Learn how to develop yourself as a leader and activate teams that deliver game-changing results.

Winning in cybersecurity starts with great leaders – exceptional people that possess the unique combination of “hard” and “soft” skills that can unlock massive gains. In this book, we’ll dissect how to enable the science of cybersecurity through the art of leadership: cultivating passion in others, enlightening and rallying a broad stakeholder community, orchestrating resources, and implementing real security in an environment.

- **Start with yourself before changing the world —** understand what it means to be open to feedback, empower others, and embrace life-long learning
- **Cultivate the right vision —** discover how to build a long-lasting following by employing applied psychology to inspire, grow, and align cyber talent
- **Change hearts and minds —** see how to enable tangible progress, turn obstacles into opportunities, and develop mental harmony with a wide-ranging community
- **Structure and choreograph resources —** learn how you and your team can serve the business with the greatest agility and effectiveness
- **Implement the principles —** understand lessons learned and be the cyber leader that your organization and the world need

ABOUT THE AUTHOR

Matthew Doan is a practice lead and cyber strategist at Booz Allen Hamilton, advising senior cyber leaders across industry on how to build world-class programs and bring exceptional value to their business. His passion is for solving problems at the intersection of technology and human dynamics. Matthew is also a Cybersecurity Policy Fellow with New America.

ISBN 978-0-9990354-9-8
9 780999 035498

Booz | Allen | Hamilton