

AGILE • COMPETITIVE • EFFICIENT • ACCURATE • FASTER • PROFITABLE

The background of the cover features a dark blue gradient. In the lower-left corner, there is a vibrant display of fiber optic light trails, with colors transitioning from red and orange to yellow and white. On the right side, a blurred image of a hand pointing towards the center is visible, overlaid on a semi-transparent rounded rectangle.

ACHIEVING DIGITAL TRUST

THE NEW RULES FOR BUSINESS AT THE SPEED OF LIGHT

JEFFREY RITTER

This book is simply essential reading for corporate executives—and leaders of all kinds—in the digital age. Responsible and respectful stewardship of data and digital assets is the new corporate social responsibility. Through this book, Jeffrey Ritter continues to guide us through this amazing age of transition and opportunity, to better outcomes for companies, institutions, and, most importantly, individuals.

NUALA O'CONNOR,
President & CEO,
Center for Democracy & Technology

I don't know why Jeffrey came back from the future to teach us how to adapt to what's coming, but he did, and I am grateful. Thank you, Jeffrey.

PETER E. SAND, ESQ.,
Executive Director of Privacy,
MGM Resorts International

Jeffrey's ability to explain novel concepts is nothing short of extraordinary. In one two-hour lecture on payment systems, he not only expanded my understanding of digital trust and systems, but favorably altered the course of my future as a lawyer in a new direction. His thought-leadership in this space will transform the dialogue about governance in a digital world.

JULI GREENBERG,
Senior Vice President and Assistant General Counsel,
Citi Retail Services

Jeffrey has been, and continues to be, at the vanguard of connecting technology and the rule of law, always passionate and thinking globally. His book is a valued contribution toward our collective efforts to achieve digital trust across the cloud.

JIM REAVIS,
CEO, Cloud Security Alliance

Achieving Digital Trust should be the dog-eared companion for any intrepid entrepreneur or innovator who wishes to achieve the ever elusive key ingredient in their business or personal life—trust. The methodologies and strategies in this book build upon the human and emotional aspects of trust and create the path toward the possibility of actually achieving a sustainable digital infrastructure. If trust, as Jeffrey presents, can be viewed as a “chain of decisions,” the first decision should be clear—acquire and consume this book!

MICHELLE FINNERAN DENNEDY,

Vice President, Cisco Systems,
Founder of The iDennedy Project,
and co-author of *The Privacy Engineer’s Manifesto*

Trust, accuracy, and context are everything when it comes to Veri-feed’s success in translating insights from millions of social conversations into profitable and powerful outcomes. Jeffrey has created tools and insights that I know are game-changers for those companies and causes who know that building digital trust will spell the difference between profit and loss, fame or shame.

MELINDA WITTSTOCK,

Founder and CEO, Verifeed.com

Jeffrey’s ground-breaking ideas fundamentally challenge the assumptions that underpin risk management and open the doors to a radically new way of looking at security—built on analysis and quantification of trust. This is a must-read for any security professional wanting to engage in shaping the future of the digital world.

DR. DAVID J. KING,

Visiting Fellow, Kellogg College,
University of Oxford

Jeffrey’s treatise (and I don’t call it that lightly) is a fascinating new view on trust and risk. This book matters not just to information security professionals or any other branch of IT, but for any professional where decision-making on less than complete information is required—in other words, all of us!

DAVID MORTMAN,

Chief Security Architect
and Distinguished Engineer, Dell

For the 25 years I have known him, Jeffrey has been a visionary, always staking out new approaches on the law and technology. This new book continues his quest to bring lawyers, corporate executives, risk managers and board members into the brave new world of digital trust. His unique paradigm breaks new ground and provides us with the opportunity to view our existing and future landscapes with new eyes. With *Achieving Digital Trust*, Jeffrey has cemented his legacy as a brave and revolutionary thinker in this amazing new world.

LAWRENCE J. CENTER,
Assistant Dean,
Georgetown University Law Center

From the Board Room to our modern day asymmetric battlefield, Jeffrey Ritter's *Achieving Digital Trust* will open eyes. It provides us with a reference model that management and software architects have been seeking. The survival of the Internet as we know it is currently at stake. This book provides a look into the transparency of «Trust Decisions» and how ensuring digital truth will shape our global governance for decades to come.

PETER L. HIGGINS,
Managing Director & Chief Risk Officer,
1SecureAudit

Those things that no one wants to face are those most in need of attention. Trust is one of those things. Jeffrey provides a unique perspective on trust as a human value that has the potential to rock the structures of all our relationships in a humbling way that is overdue. This book is about digital trust, but so much more!

TRISH WHYNOT, D.C.ED.,
Author, Counselor

Jeffrey is a global authority on digital trust. He is one of the few people that understands where information security, risk and law converge, where they are headed and how they relate. This book breaks new ground and is a must-read for boards of directors and executive teams.

BOB WEST,
Managing Director, Careworks Tech

Ten pages into this book, you'll understand why author Jeffrey Ritter is described as "passionate," "inspiring," and "visionary" by his students at Oxford, Johns Hopkins and Georgetown. He embraces this topic of digital trust in all of his work and eloquently gets across why we should care about it. His book empowers us to know what we can do to keep ourselves and our organizations safe in cyberspace. Read it and reap.

SAM HORN, CEO of Intrigue Agency
and author of *Tongue Fu!* and *Got Your Attention?*

Civility begins with trust. In this digital world, Jeffrey Ritter has taken on the challenges of building and achieving trust with remarkable insight. His tools enable all of us, regardless of our roles, to collaborate, communicate and work together more effectively. *Achieving Digital Trust* empowers you to work, live, and thrive with greater civility and an enhanced level of professionalism.

SUE JACQUES,
The Civility CEO® and author of *What The Fork?*

As a landscape architect, I know the challenges of identifying, synthesizing, and navigating all of the rules required to create something functional, aesthetic, and valued. In this book, Jeffrey Ritter is giving all of us new tools with which to design, build, and use digital assets within the vast complexity of cyberspace. This is an exciting contribution to the architecture of our world.

BIBI GASTON, Landscape Architect
and author of *The Loveliest Woman in America: A Tragic Actress,*
Her Lost Diaries, and *Her Granddaughter's Search for Home*

ACHIEVING DIGITAL TRUST

ACHIEVING DIGITAL TRUST

THE NEW RULES FOR BUSINESS AT THE SPEED OF LIGHT

JEFFREY RITTER

***Achieving Digital Trust:
The New Rules for Business at the Speed of Light***

©2015 by Jeffrey Ritter

Library of Congress Cataloging-in-Publication Data

Ritter, Jeffrey

Achieving Digital Trust: The New Rules for Business at the Speed of Light / Jeffrey Ritter
p. cm.

ISBN: 978-0-9965990-0-9

Printed in the United States of America

22 21 20 19 18 17 16 15 |CS| 10 9 8 7 6 5 4 3 2 1

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, or by any information storage and retrieval system, without permission in writing from the author. The corporate names of AT&T, Boeing, Chase, eBay, Google, Home Depot, JP Morgan, The Limited, Sony, and Target are registered trademarks of those companies. The characters and other company names used to illustrate principles in this book are fictional and bear no resemblance to persons living or dead or companies.

Editorial development and creative design support by Ascent:
www.itsyourlifebethere.com

Design by Peter Gloege | LOOK Design Studio

Graphic illustrations by Paul McTaggart

Content editing by Jane Kuhar and Lee McIntyre

Follow Jeffrey Ritter:

www.JeffreyRitter.com  [jeffrey.ritter52](https://www.facebook.com/jeffrey.ritter52)  [@Jeffrey_Ritter](https://twitter.com/Jeffrey_Ritter)

This book is dedicated to my daughters,
Jordan Michelle and Chelsea Marie,
and their inspiring passion to make this a better world.

TABLE OF CONTENTS

PREFACE: The War on Trust	13
---------------------------------	----

THE TRUST DECISION MODEL—PART I

1: The Global Demise of Risk Management.....	31
2: The Power of Trust	45
3: The Trust Decision Model from 40,000 Feet.....	59
4: Context Is Everything!.....	79
5: Describing the Circumstances and Resources	103
6: Classifying Resources	127
7: Drawing the Lines	161
8: Defining Work.....	179
9: Time, Money and the TDT.....	217
10: Dancing the Tango of Wealth and Trust	251
11: T Minus and Holding.....	275

DESIGNING DIGITAL TRUST—PART II

12: Introduction	289
13: Facing the Challenge of Digital Trust	293
14: The Velocity Principle.....	303

15: Bridging the Chasm of SIAM.....	333
16: The Rules for Composing Rules.....	357
17: The Digital Trust Design Principles	379
18: The Unified Rules Model	393
19: The Unified Information Model.....	441
20: Creating Wealth with Digital Trust.....	465

MANAGING & GOVERNING DIGITAL TRUST—PART III

21: Achieving and Sustaining Digital Trust.....	487
22: Achieving the Outcomes	491
23: The Trust Prism	501
24: Using the Trust Prism	527
25: Entering the War and Winning the Revolution.....	537

APPENDIX: Trust Decision Tools.....	549
GLOSSARY: Trust Vocabulary Terms	555
References and Additional Sources.....	565
Acknowledgements	571
Author Biography.....	576



PREFACE

THE WAR ON TRUST

ACROSS THE WORLD, daily headlines confirm there is a global war for control of digital information. The targets are immense—Sony, Target, Boeing, JP Morgan, Chase, Home Depot, AT&T, eBay, Google, power utilities, airlines, and virtually every governmental agency in any nation. The targets are small—your credit card, your browsing history, your calls for taxi services, your health data, and your preferences for beer.

This war is being shaped by weapons of attack we have heard about—Stuxnet, Backoff, DDoS, Gauss, malware, sniffers, and eye-glasses that film you punching in ATM passwords. This war is being shaped by weapons of attack that have yet to be created, designed to exploit the weaknesses and vulnerabilities of new technologies that, themselves, have yet to be invented.

The objective in this war is simple—to gain control of the digital knowledge assets each of us seeks to use in the decisions we make every day:

Important decisions like picking the best schools for our children or choosing the doctor to perform life-altering surgery.

Small decisions like finding the gas station with the best prices.

“Bet it all” decisions that place a nation, a company, a division, an employee team, or the wealth saved across generations at risk—the decisions that leave you sweating bullets and not sleeping.

When the information you need to make decisions is controlled, the quality of your decision is controlled and the possible outcomes from which you can choose slip from your control. Where there is less information, your decisions become vulnerable. As an executive, an IT architect, an investment manager, an educational director, or even a parent, your job is to lead with good decisions. You want your decisions to be ones that others will follow. But those ambitions erode when those fighting the war to control digital information are winning.

In reading this book, you will explore and acquire an entirely new portfolio of tools and strategies to help shift the momentum of that war. As in any combat or battle, to succeed, it is essential for you to understand what is at stake. What we are facing is more than a war to control information. It is a war on our ability to trust information. Yes, a war on trust.

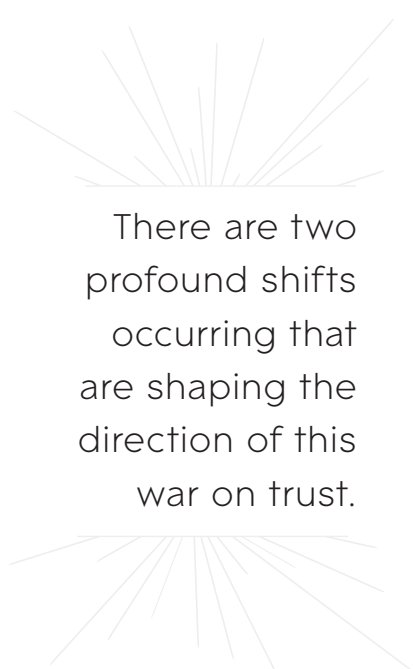
At every turn, you can sense that, somehow, the critical fabrics of trust that have been woven together for thousands of years and that allow us to live in social systems are unsteady, trembling, and fragile. It is as true in our national governments, corporate

boardrooms, and compliance programs as it is in our interactions with sales clerks and neighbors. Decisions you take as a leader are questioned more intensely. As a team member, business analyst, armchair investor, or family financial officer, you have become more reluctant to accept the decisions of others. Blind faith is no longer an acceptable justification to lead others in a charge over the hill, or a basis on which you choose to follow others. Why is trust under attack at so many levels, across so many economies, and in so many routine, ordinary decisions through which we live our lives?

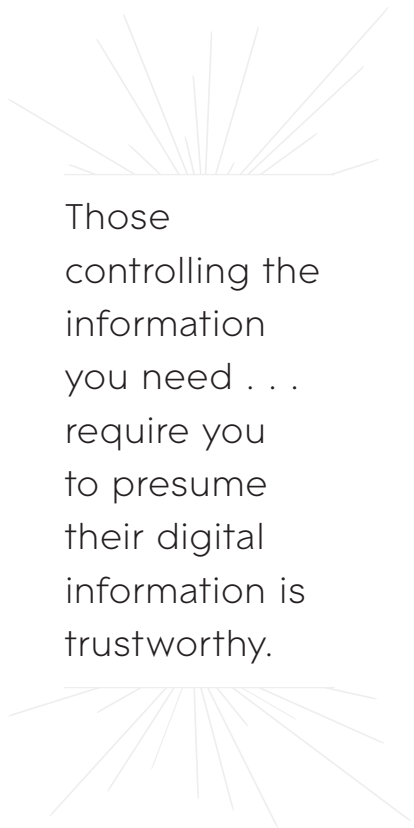
THE CURRENT PLAYING FIELD

The Internet, the embrace of cyberspace, and the ubiquitous presence of digital information in human society are making immense, positive contributions. In the simplest actions of our daily lives and in the most important decisions we make in business, in government, in education, and in choosing between war and peace, we have become reliant upon the availability and presence of digital information. As our reliance speeds into dependency and, in turn, addiction, there are two profound shifts occurring that are shaping the direction of this war on trust.

First, technology is compressing the time we have to make good decisions. The immediacy with which information can be accessed, the speed of communications, and the competitive pressures to make decisions NOW are carving tighter decision-making deadlines into everything we do. Automation is requiring you to make decisions faster. Global competition makes each decision you execute more consequential. The pressure to get to the next decision is exacerbated by the ease with which technology places information for the current decision at your fingertips.



There are two profound shifts occurring that are shaping the direction of this war on trust.



Those
controlling the
information
you need . . .
require you
to presume
their digital
information is
trustworthy.

As a result, to act within the time constraints of deadlines, the presence of fiercer competition, and the looming threat of higher lost-opportunity costs, you have no choice—you must *presume* the trustworthiness of the information you acquire to make decisions. Deciding now requires you to acquire the information you need from the most accessible source, with zero time to ask the important questions: “Where did this information come from? Who put this report together? Has the data been confirmed to be accurate? Who actually authored the analysis? Is the history you are teaching my children objective? Does this bank statement reflect all of our deposits?”

Answering these types of questions is inherent to how we make good decisions. You seek information that serves as fuel for your decision. You work hard to validate that the information can be trusted. You calculate toward your decision, constantly evaluating whether the information holds up its reliability. But in today’s 24/7/365, wired decision-making landscape, there is no time to ask those questions. Those controlling the information you need understand that pressure and require you to presume their digital information is trustworthy and reliable for making your decisions. Thus, to gain control of digital information is to succeed in imposing an enormous handicap—removing your ability to challenge its trustworthiness by asking the right questions.

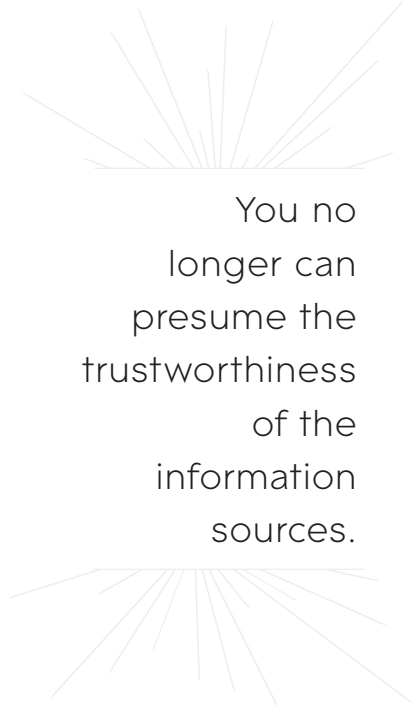
Second, information technology has rapidly created a different kind of infrastructure through which information and knowledge can be stored. The Net is a global facility that never was designed for how we now use it—as a primary and essential repository for the knowledge of human experience. Cloud-based services, distributed storage systems, and server farms on every continent—all are locations in which the information you need for your decisions

may be found. Yet, the custodians who operate these facilities are not the public library or local university; instead, a mind-boggling inventory of multiple, connected networks of service providers, application providers, contractors, sub-contractors, and agents—both human and automated—interconnect to support the global appetite for information through agreements, contracts, terms of service, and other rules of play into which you have had no input and the details of which you may never have knowledge.

In the 20th Century, companies kept their information assets under lock and key. In science, libraries curated and archived information and validated the authors and the bases of their research. Governments were trusted to preserve and keep accessible the vital records of those they governed. When you sought out information, you could trust the source. Today, that is the second shift—you no longer can presume the trustworthiness of the information sources. Indeed, you not only are asked to presume their reliability as sources of information; you also must presume their security as custodians engaged in collecting the surveillance, monitoring, and behavioral data about you, your family, and your company.

These two shifts are inexorable and serve as the best evidence of the momentum of the war. As the headlines now report on a daily basis, neither trust in digital information nor trust in the sources and custodians of digital information can be presumed.


For those of us who are decision makers, these are huge problems. With growing velocity, we are losing our ability to trust digital information to be factual, accurate, reliable, and authentic. But we also are losing something far more important—trust in the quality of our own decisions and our confidence in those we trust to make good decisions.




You no longer can presume the trustworthiness of the information sources.

THE BREAKDOWN OF TRUST

Whether in government, in business, in classrooms, or at the dinner table, the ubiquitous presence of digital assets and devices enables us to do something radical—immediately seek out information that allows us to challenge and evaluate our trust in the decisions of others we are expected to follow. So, in addition to your own decision process being shaken, so too are the evaluations others make to trust your decisions. If you are a business leader, IT executive, information security manager, systems architect, elected public official, educator or stay-at-home parent, you have surely felt the discomfort.



As soon as you announce a decision, someone is thumb-typing on a device to find information to validate or contradict you.



As soon as you announce a decision, someone is thumb-typing on a device to find information to validate or contradict you. A few clicks and your questioner has acquired data that enables that person to challenge your decision process, view it differently, or weigh it with less confidence. Admit it, you surely have done the same when you are on the other side of the table, hearing the decisions, opinions, or guidance of others—a superior officer, a corporate manager, a business partner, a teacher, or even a spouse.

Technology is empowering us with accessibility to information but undermining our effectiveness in how we use information to make decisions. The Net is delivering unprecedented immediacy in how we communicate decisions to our teams, yet empowering them to question the qualities of our decisions and, in turn, hold back their trust until they do so. We are at a tipping point that is very different than previously imagined. Rather than tipping forward in mass market adoption, we are somehow struggling, wavering, and uncertain about the directions in which to move.

It is really very simple. In the foreseeable future, we will not function as a global society without the Net and the immense digital resources and information assets of our society. The addiction is established—commerce, government, education, and our neighbors offer no option other than to require that we rely upon digital information in making decisions. But we will not function successfully if the war for control of those assets is lost. The battlefield, however, is the one on which trust is to be gained or lost—trust in the information we use, trust in the infrastructures that support us, and trust in the decisions we make in a digital world.

If we are to turn the tide in the war for control, and prevail in maintaining a digital infrastructure through which we can sustain societies and a functional, global economy, we must design and achieve trust in the digital information we use, trust in the infrastructure of the Net through which we live, and trust in the decisions we make in a digital world—we must build what I call *digital trust*.

WHAT IS DIGITAL TRUST?

Some years ago I began to study how we place our trust in digital things—networks, computers, systems, applications, and, of course, the information that is both the fuel and the output of their operation. In pursuing an understanding of digital trust, I learned that two far more difficult challenges first had to be conquered—I needed to figure out how we, as human beings, *decide* to trust, and I had to figure out how any of us makes decisions that *can* be trusted.

The questions rose up and multiplied:

Is trust just an emotion, a feeling that we sense and use like a crude compass to find our way from here to there?

How do we decide to trust the people in our lives, the tools we choose to perform our work, and the information we consume, whether in business, education, or entertainment?

How do we choose our employers or employees, supporting financial institutions, board members, or our governments?

How do we calculate the value we will pay for the products, services, and resources in which we place our trust every day in order to live our lives?

How do we lose trust in something or someone?

How does a leader gain the trust of those following, and how can that trust be lost?

Is trust merely the condition in which we live when we are not in fear of known risks, a default setting that is hard-wired into how we think?

Uncovering the answers to those questions about how we decide to trust, and how we make decisions that can be trusted, came first. Only then could I proceed to ask and try to answer the additional, increasingly complex questions about how we might build and achieve *digital trust*.

What changes when you are deciding to trust a machine, a mobile device, a game, or a business application?

How do you decide to trust digital information that is intangible and cannot be lifted, opened, or flipped through?

What questions do you need to ask to conclude that trust is justified in both digital information and the sources from which you acquire the information?

How do you make trust decisions about people, associations, tools, or their value when the information upon which you will rely is increasingly digital and intangible?

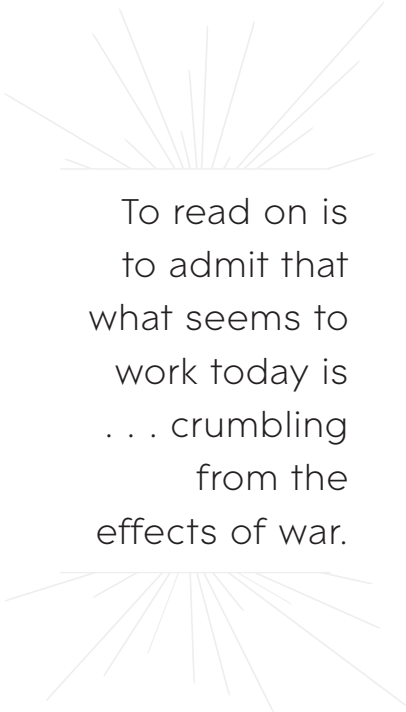
In a global culture in which digital trust is under attack and degrading, how can you build and engender old-fashioned human trust with your customers, business partners, associates, and employees?

Flooded with digital information, devices, and the capacity for others to question decisions, how can you make better decisions, choose the superior alternatives, and reduce the number of decisions that “just take the risk” because of data that is missing or not proven to be reliable?

Can achieving digital trust be proven to be good business and create new wealth in a global, 24/7/365 marketplace that demands increasing velocity while also increasing the risks of living digitally?

This book presents the answers—the right answers—to those questions. In doing so, these pages help you understand how to

demand and build authentic trust in the digital information and the devices, systems, and networks of the Net you access to do your job. Certainly this book will empower you to be more successful at building and delivering digital information devices, applications, and data assets that gain the trust of all of the stakeholders with greater velocity and increased value. But this book also will help you to craft and execute your decisions differently and more effectively in a digital world.



To read on is
to admit that
what seems to
work today is
. . . crumbling
from the
effects of war.

Whether in business, science, education, finance, or at the family kitchen table, each of us is a leader to whom others look for guidance and support. If you are prepared to invest your time to learn the insights, principles, tools, and strategies assembled in these pages, you and your decisions will be more trusted.

Doing so will require a bit of courage on your part; after all, to read on is to admit that what seems to work today is, in fact, crumbling from the effects of war. Yet to deny that the war is underway is not a viable option.

WHAT IS IN THIS BOOK FOR YOU?

In *The Trust Decision Model—Part I*, you will acquire a new way of thinking about how trust decisions are made. You will learn about all of the moving parts in trust decisions and how to view them differently. You will be introduced to new tools that allow you to better navigate the interaction of those parts and, in doing so, to improve your control of how your decisions earn the trust of others.

If you lead a team, these new tools will strengthen
how you structure and execute the tough decisions

on which your company, and your ability to lead, are on the line.

If you take responsibility for auditing or testing how well decisions are being made, these new tools will enrich the questions you ask and the answers you deliver to those who are counting on you to watch their backs.

If you want to elevate the trust with which your decisions are accepted, these new tools will improve your ability to communicate how you reach your decisions and how you collect and process the information required.

In *Designing Digital Trust—Part II*, you will learn how to design and build *digital trust*. You will have the opportunity to expand on your knowledge of trust decisions and be introduced to additional new tools to build, select, and create wealth from trusted digital assets.

In *Managing and Governing Digital Trust—Part III*, you will discover that building digital trust is not enough; to survive and prosper, you must sustain and improve digital trust. The strategies and tools to do so are uncovered, together with recommendations for the next steps to be taken.

If you design technology or digital solutions, this book will transform how you build those solutions and achieve greater effectiveness in the design, development, and operation of your work product.

If you manage a business, whether at the family kitchen table or in a corner suite in one of the world's tallest buildings, this book will change how you define and shape your strategies to create new wealth, compete, and survive in a world that soon will be only one digital marketplace.

If you select and use digital assets (and, among us, who does not?), this book will give you new mechanisms for making better decisions when selecting among your options, taking into account the trade-offs among trust and risk, and the wealth to be created (or lost) with each.

If you are reading this book as a regulator, lawyer, or policy geek, this book will alter how you will perform the responsibilities of authoring and administering the rule of law in the Digital Age.

Despite decades of research on organizational trust, behavioral sociology, marketing, artificial intelligence, user interfaces, and human relationships, the vocabulary and tools needed to build digital trust simply do not exist. So, within these pages, I share with you a new portfolio of tools and resources:

PART I

A Trust Vocabulary, composed of new phrases and terms and new meanings for existing words (with appropriate acronyms and symbolic notations), which enables us to discuss trust decisions and digital trust differently and with greater effectiveness.

A Trust Decision Model, an integrated view of the sequential decisions and information layers that link together the steps we take in

deciding to trust and enable us to connect the dots between human trust and computational trust.

PART II

The *Rules for Composing Rules*, a set of eight simple principles for authoring rules that are effective when crossing the chasm between the ambiguity of broad, governing rules (such as statutes or regulations) and the binary precision required by the executable code of software applications.

A *Unified Rules Model*, a new architecture that enables us to organize all of the complexity of business, technology, and legal rules into unified, functional structures that support the design and execution of digital systems that truly deliver compliance and earn our trust.

A *Unified Information Model*, a new framework for organizing and designing digital information assets in order to execute more effective trust decisions and perform more effective governance.

PART III

The *Trust Prism*, an entirely new, 3-D, visual tool for evaluating, improving, and governing complex information systems and information assets. The Trust Prism unleashes our potential to build and sustain digital trust in those systems and information assets for enduring generations.

Ultimately, I hope this book will contribute to global dialogues about how we will govern ourselves. In these opening decades of the Digital Age, the world is one. Very shortly, there will be no further emerging markets. The boundaries of our political states

already have become secondary to the boundaries of our networks and our systems, and the economic wealth we hold in our wallets and bank accounts is becoming secondary to the value of the digital information we can access and control.

Only the digital information that we truly can trust will have such an impact. If we cannot resolve how to tell the difference among digital assets we can trust and all of the rest, and if we cannot author rules that can be enforced globally by both nations and systems, the global dimensions of the Internet will collapse, national boundaries will become new Berlin Walls, sponsored acts of digital terrorism will become routine headlines, and the potential of these amazing technologies to bridge the chasm between man and machine will not be realized.

In early 2015, during the final development stages of this book, senior executives from Microsoft, Cisco, and Salesforce.com were speaking at global forums about the need to build digital trust and the economic costs of recovering from a loss of trust. The EU is committing vast resources toward building competitive digital markets. Yet the digital infrastructure that now runs our world—despite all of its capabilities and services—is broken. History has always confirmed there is a time when existing infrastructures can no longer merely be patched and kept in service. I believe any further patching of what now exists will fail; instead, something new must be designed.

WE CAN WIN

If we are to prevail as a *civil, global* society, designing and achieving digital trust is now a necessity. We must find the courage to move beyond what seems to work today but actually is crumbling.

We must move beyond merely shoring up our defenses with stronger, more robust spending. Instead, we must begin anew, replacing what *is* with what *needs to be*—a robust, dynamic, interconnected, digital space through which we can communicate and live as a global society. In doing so, we can improve our confidence in our decisions and the decisions of our leaders.

Now is the time to accept the tremendous opportunity we have to truly build and achieve new systems and new information assets that can deliver and sustain digital trust. Welcome to taking the first steps to shifting the tide and winning the war.

PART ONE

THE TRUST DECISION MODEL



CHAPTER 1

THE GLOBAL DEMISE OF RISK MANAGEMENT

I COMMITTED A LONG TIME AGO that any book I would write on digital trust was not going to begin with an endless tirade of how bad things are in cyberspace. There is simply no need; the daily headlines from the digital battlefield are enough. Google (or your search engine of choice) can provide you with abundant stories of the continuing sophistication with which malicious actors are achieving victories in the war to degrade our security protections on information and gain access to the digital knowledge, records, and controls that we most value. There are detailed reports, surely more than your appetite can sustain, explaining the economic and operational impacts of hacks, criminal syndicates, espionage, and state-sponsored take-downs of entire networks and systems. All seem to be compelling evidence of the fact that digital trust is under attack.

Yet, before we journey on, you deserve to know that not a single commercial publisher presented the opportunity to publish this

book elected to do so. The reasons, remarkably consistent across nearly a dozen discussions, included:

“We don’t sense there is a ‘felt need’ to which your book responds.”

“Building and sustaining digital trust does not seem like a hot button topic; no one else is writing about it.”

“Your book is too broad; none of our subject editors (Technology, Security, Public Policy, Sociology, Law) saw a good fit.”

Somehow all of the headlines did not have any impact. Indeed, one anecdote gave ironic support to their failure to be persuaded. In late 2014, after more than 10 years of existence, the Trustworthy Computing Initiative within Microsoft Corporation was closed, with its team members distributed across other divisions or laid off.

As mentioned in the Preface, however, in early 2015 (and after the publisher rejection notices had accumulated), things seemed to be changing.

» At the 2015 World Economic Forum in Davos, Marc Benioff, the CEO of Salesforce.com observed:

“The digital revolution needs a trust revolution. There has been an incredible shift in the technology industry. . . . We’ve gone from systems of record to systems of engagement and now we are about to move into a world

of systems of intelligence. But none of these will retain form or have referential integrity unless the customers trust them.

Trust is a serious problem. The reality is that we all have to step up and get to another level of openness and transparency.”*

*<http://bit.ly/1eQ23BK>

- » The White House organized a Summit on Cybersecurity and Consumer Protection in February 2015, which the President personally attended.
- » The European Union has recognized digital trust as an essential pillar in their overall Strategy for a Single Digital Market.
- » Global, rising technology companies are establishing the new executive role of Chief Trust Officer.
- » The Cloud Security Alliance, a new professional association with thousands of technology professionals and hundreds of corporate sponsors, is authoring and publishing new protocols for achieving trust across the global complexity of Cloud services (and a portfolio of acronym-defined services: PaaS, IaaS, and SaaS).
- » At the University of Oxford, the Department of Computer Science includes professors and students focusing on trusted computing and trusted infrastructure, with an emphasis on Cloud-based distributed computing systems.

» In China, in September 2014, the 13th Annual Conference on Trust, Security, and Privacy in Computing and Communications was convened, with over 100 papers presented. Held under the auspices of the prestigious IEEE, what is intriguing is the frequency with which an international conference of this calibre is so frequently held in China and the strong, diverse contributions from Chinese and Asian researchers (as opposed to U.S.- or European-dominated programs).

Let me emphasize the last example—13th annual! Yet another is scheduled in 2015. There is an obvious passion in China toward building digital trust, one that seems reaffirmed with each new conference. Given the level of investments in research reflected by the papers and attending organizations, authentic momentum and progress are being achieved. Each year the volume of contributions, the sophistication of research, the diversity of topics, and the structural complexity of the Conference are richer. Here are just four recent examples: “Public-Key Encryption Resilient against Linear Related-Key Attacks Revisited”; “A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment”; “To-Auth: Towards Automatic Near Field Authentication for Smartphones”; and “Proofs of Ownership and Retrieval in Cloud Storage.”

Citations and links to materials appear in References and Additional Resources at the back of this book.

CHINA TAKES THE LEAD

This event is more than just another throwaway “angels dancing on heads of pins” conference, and the strong, continuing contributions from Asia are not merely coincidence. China, as an economy, research center, and population mass, clearly recognizes value in pursuing and advancing digital trust. The annual event has another benefit—vacuuming into one collection point the scientific papers, emerging corporate best practices, and published innovations of researchers and entrepreneurs from the world’s most recognized universities and companies, as well as those across that nation’s own vast resources.

Five compelling principles explain this Chinese momentum on trust. Yet there is nothing *digital* about them. Each is proven to influence economics, social organizations, governance, and human behavior. Each has guided the destiny of commerce for centuries, determining the outcomes of countless battles for investor capital, product innovation, consumer choice, and, ultimately, control of market share.

Shaped long before Alan Turing, the first research grant that funded the Internet, the first protocols of the World Wide Web, or the birth of an Internet of Things, these principles have consistently marked the winners in human society. Yet we are only now realizing what the Chinese understood in hosting the earliest conferences on digital trust, security, and privacy at the beginning of this century—in the next generation of the Digital Age, the winners will be distinguished from the losers by these principles.

Every transaction creating wealth first requires an affirmative decision to trust.

Building trust creates new wealth.

Sustaining trust creates recurring wealth.

Achieving trust superior to your competition achieves market dominance.

Leadership rises (or falls) based on trust (or the absence of trust).

Take a moment and think about each of these with respect to what you do in your business or in your job. How does the organization acquire wealth? Where does new wealth originate? How are customers retained? What provokes them to keep coming back and paying for your goods or services? Why does the leader in your market succeed? If you are not the market leader, why not? How is the loyalty of your team maintained?

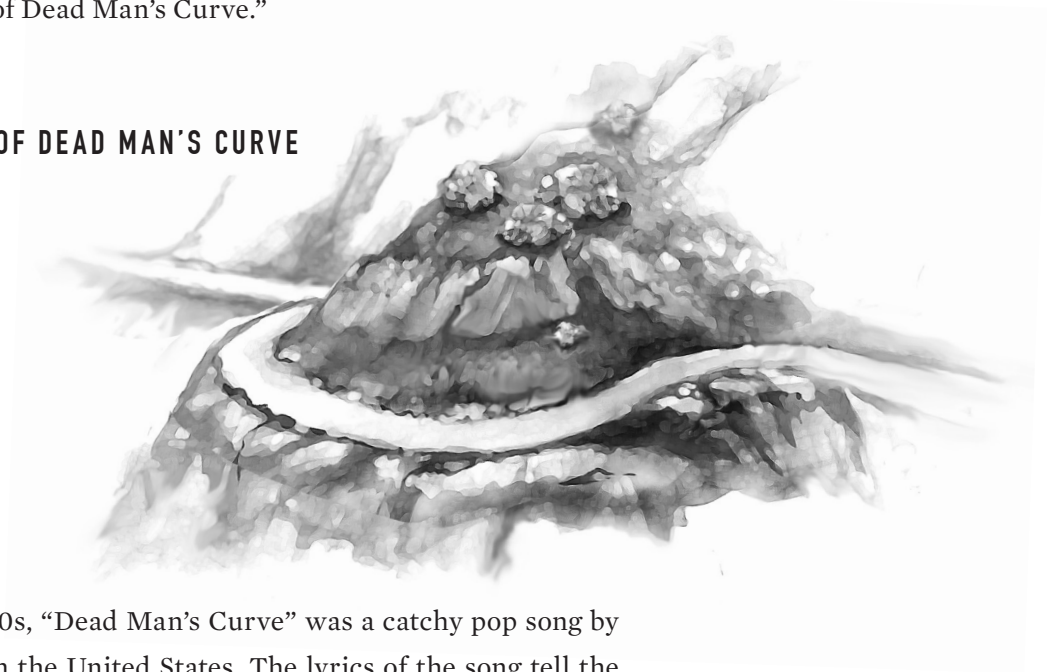
If you lead a non-profit, a government agency, or even a community association, your focus is only slightly different but the trust is often harder to earn. You still require sponsors, funding sources, and need those you serve to place their trust in your organization and your leadership. But the direct exchange of value between a buyer and seller is not present. What must be done to secure the trust of your funding sponsors? How is your success measured when renewed funding is requested? How are you effective at leading change when, quite simply, you are not able to pay the same as the private sector? If there are options—whether for funders, those you serve, or both—how do you compete against those options? What is required to secure their trust?

For both profit and non-profit, whatever provokes funding sources to trust seems to drive everything. Trust surely will have the same

determinative force within the broad expanse of the Net and its networks, systems, devices, and the full portfolio of the digital information assets of humanity. Yet, why did the publishers not see the critical importance of *digital trust*? Why have the technology leaders from North America taken over a decade to catch up (if only in their rhetoric) to the investment China has been making in figuring out the building blocks needed to achieve digital trust?

I suggest they are caught in a *Twilight Zone*-like episode called “The Dilemma of Dead Man’s Curve.”

THE DILEMMA OF DEAD MAN’S CURVE



In the early 1960s, “Dead Man’s Curve” was a catchy pop song by Jan and Dean in the United States. The lyrics of the song tell the story of a dare, a green light, a race to Dead Man’s Curve, and a hideous crash. There actually was a real Dead Man’s Curve, part of the Old Timber Road in California, a tight, 270-degree curve and switchback with no berms and steep, unguarded drop-offs. It demanded slow and careful navigation . . . or else. But it was a road, a superior means of transit to get from here to there than what had existed before.

The road itself was just that, nothing more. It worked in earlier years when the number and speed of cars and trucks were both few and slow. But as the velocity of cars increased and more drivers of younger age took the wheel, there really were multiple crashes and deaths—wheels slipping off the edge as the laws of physics overcame foolhardy bravery (often fueled by fermented fluids), or head-on collisions between cars driving blind to approaching vehicles on the other side of the curve.

Yet, despite the losses of life, rather than replace the infrastructure the road represented, the government continued to take the risks. The road remained in use. While there is no historical record I could find, we can only imagine the budget meetings and improvements discussions over time.

“Perhaps we can put up wooden guard rails.”

“No, it will be cheaper just to post a warning sign on both sides of the curve.”

More kids died.

“Perhaps we need to put up metal guard rails; I saw them being used in Chicago on a new bridge.”

“No, too expensive. But let’s put in the wooden guard rails we talked about last year.”

But the cars were even bigger, the motors stronger, and the drivers a bit more reckless, crashing through the wooden guard rails. More kids died.

“We have so many cars and trucks now using the

Curve, perhaps we should just blow that rock out of there and straighten the road.”

“Our road budget is fairly tight; perhaps we can replace the wooden guard rails with the metal fencing you saw in Chicago.”


Still more kids died.

The Dilemma of Dead Man’s Curve is this: when the existing infrastructure no longer supports the demands placed upon it—causing injuries, loss of life, disruptions of operations, etc.—the operators of that infrastructure always will try to mitigate the related risks by installing patches at the lowest possible cost. Their goal is to extend the useful life of the investment in the infrastructure, despite the expenses of losses that may result. Patching Dead Man’s Curve is always lower in cost than investing in building a new, functional infrastructure. But the patches merely delay the issue—when should we decide to abandon what exists and invest in building something new that will work?


THE INTERNET IS A DEAD MAN’S CURVE

The Internet, for all of its power and unexpected capabilities, is merely a digital version of the Old Timber Road. It originally was envisioned as a military communications infrastructure to move messages, resembling an electronic interstate highway system. The Internet was never designed to support the full demands of the global human population for commerce, government, warfare, entertainment, intelligence, knowledge, education, online dating, and homeowner association newsletters.

In the headlines and in our daily interactions with the Net, more



Patching Dead Man’s Curve is always lower in cost than investing in building a new, functional infrastructure.

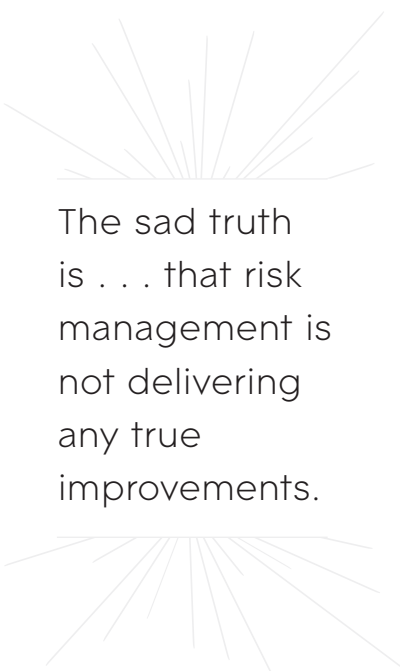


and more we see the debates over what spending is needed and how the Net is outgrowing our ability to govern it. Yet, in corporate board rooms, IT spending plans are no different than the budgets presented to the county supervisors overseeing Dead Man's Curve—asking for money to patch, rather than to build new.

We hear the sounds of alarm; we become direct victims of identity theft, credit card fraud, and the unauthorized publication of personal photographs. Our corporate websites are compromised, financial accounts hijacked, and trade secrets and intellectual property digitally stolen. And yet, rather than invest in building something truly new and functional, we continue to justify spending on patching. Time and time again, the prevailing votes are cast based on the perception that spending on patching will best protect the wealth of the organization.

In contemporary consultant-speak, there is another term used to describe the continuous patching of existing infrastructure: “risk management.” The sad truth is, of course, that risk management is not delivering any true improvements. The infrastructure is merely being patched. While the demands for service and the pace of commerce gain velocity, so fast as to be measured in nanoseconds, there are still disrupted transits of data, dropped packets, and recurring major system breaches.

The reason risk management fails is simple and fundamental. There is only one source of funds for risk management—the net profits of the organization after all of the other production and management costs have been paid. Spending for reducing risk is never connected to how customers make their trust decisions to buy the goods or use the services of a business. It is always viewed



The sad truth
is . . . that risk
management is
not delivering
any true
improvements.

as a deduction against profits, spending to be minimized or avoided altogether by decisions to “take the risk.”

For decades, the champions of information security, records management, and compliance have battled for adequate funding. They usually lose, receiving nothing or only a small portion of the requested budgets. Why? Because the only source of funds that could be tapped were the profits, wealth otherwise traveling into the pockets of the shareholders. The battles already were lost before they began. “Risk management” is, in its essence, a simple way of saying, “What’s the lowest possible amount to be spent from our profits to reduce the risks of the existing infrastructure failing to deliver wealth to our pockets?”

In advocating a different path, I submit that risk management is failing as a business discipline; in fact, the increased rhetoric and activity for digital trust already may be the first nails sealing the coffin in which risk management will be buried.

If I am right, the publishers are going to resist. They make their money by selling lots of books, webcasts, and software products that are “patches” to manage risk. So too will the consultants, venture-funded start-ups, lawyers, and policy regulators who have great job security delivering patches. Bluntly, managing risk is very lucrative, particularly after a successful attack or theft has placed your client or customer’s management team under scrutiny.

You identify the risk, you build a defense, and you install the defense, hoping the adverse incidents go down in their volume or severity or disappear entirely. It is really no different than installing guard rails on a main road that needs to be abandoned, not

patched. The current infrastructure is being preserved, even when the demands are clear that *something new is needed*.

China understands the difference. The EU, at the highest levels of strategic planning, understands the difference. Those investing today in digital trust standards and protocols that work across the full, broad dimensions of the global society get it. Each recognizes and values the potential rewards that can be achieved if something new emerges that is superior to the status quo. New investments in new infrastructure—networks, systems, devices, applications, and information assets—that are designed to be trusted will prevail, in accordance with the 21st Century versions of the time-honored trust principles highlighted at the beginning of this chapter:

*Affirmative decisions to trust made by the market
will create wealth.*

*Building and expanding trust across more services
will create new wealth.*

Sustaining trust will create recurring wealth.

*Achieving trust superior to the competition will
achieve market dominance.*

*Leadership will be awarded to those who rise to be
trusted.*

There is one more reason why risk management is failing. The managers and champions for the spending have never been able to connect the proposed investments to how their companies can create wealth. By focusing with a digital perspective on the five principles of trust that drive economies, companies, and leadership, the dialogue changes. Now the same spending has a different

connection point—improving how companies can create and sustain new wealth. So, when China, the EU, and others begin shifting the public conversation toward digital trust, know they already made the shift internally a long time ago.

DESIGNING, ACHIEVING, AND SUSTAINING *DIGITAL* TRUST

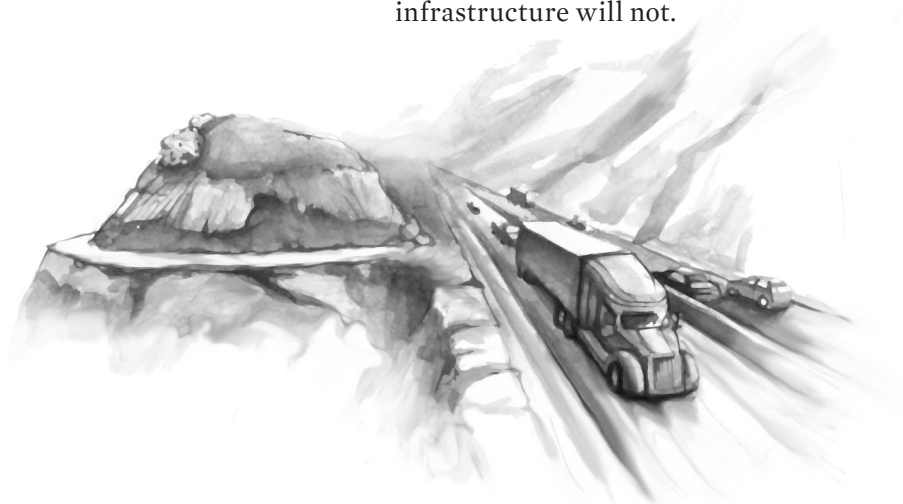
Building digital trust means investing in the architecture, design, and production of something new. The building process is one that must be continual.

Designing digital trust means researching the rules used by others to determine what products or services they will trust enough to pay value. You need to know *their rules* in order to create something new that will earn the trust of your customer, business partner, colleagues, team, or classroom. That may seem simple, but the challenge in the Digital Age is that none of us knows what those rules need to be.

Achieving digital trust means building and executing your products and services in alignment with those rules and with a transparency that enables the trust decisions of others to be made with greater speed and certainty. You must leverage the capabilities of technology to deliver to them the information they need to make their trust decisions rather than control or restrict their access to that information.

Sustaining digital trust means designing your products and solutions to be adaptive and responsive to changes in the rules. Nothing will be more important in the 21st Century than building into the design of the Net and all things digital the agility and flexibility to react quickly. Regardless of the geography, the market, or the

system that defines the playing field, it is certain in the Digital Age that *the rules will change*. The winners who survive and prosper will be those who build a flexible infrastructure and solutions that enable adaptation and responsiveness to changes in the rules. Those who continue to focus on managing risk and patching the current infrastructure will not.



It is inevitable that the existing infrastructure of the Net will end in the same fate as Dead Man's Curve. Now, it is an abandoned, overgrown stretch of crumbling blacktop that can be seen in the distance from the superhighway that replaced it. The patching ultimately stopped. New rules were built to sustain and support commerce and the higher volumes and velocities that were possible. New investments were made, transit moved more quickly, sales occurred with greater velocity, and the communities served thrived.

In the next few years, those who are first and best in achieving digital trust will become the new superhighways for a unified, single economy firing across a globally connected world. Using the resources and strategies delivered in this book, you can catch up with those who already have figured it out, and then accelerate past them. The first step is to acquire a new way of thinking about trust itself. In the next chapter, that process begins.



CHAPTER 2

THE POWER OF TRUST

TRUST CONTROLS VIRTUALLY all human behavior. At each level of interaction among people and the objects and things around us, trust is the foundation of our decisions. At some point just beyond behaviors that are purely instinctive (such as the beating of your heart or the synapses firing within your brain), each and every action with which you live your life is informed by the strength and quality of trust.

Trust is also the essential quality of leadership. Effective leaders succeed because they make decisions that will be trusted. Nothing is more powerful. Trust is achieved by making decisions that produce favorable outcomes. What matters to leadership is that those outcomes are measured against the criteria of those who are to be led. Yet trust also is incredibly fragile; a single decision with catastrophic consequences can destroy one's ability to ever again earn the trust of others. In nearly every decision we make, the most cherished asset at stake is the trust others place in our decisions:

- After 17 years of growth, the company was losing market share. Imports, shipped directly to consumers from overseas, were corroding revenues. The CEO faced a decision—to fund a new automated production line, does the company lay off 20% of their employees or merge with an overseas competitor with a new facility but no current market volume?

- Challenged to use Cloud-based services to reduce operating costs, a CIO must select between three competing vendor proposals, none of which delivered the performance reports required to evaluate their remediation response times. Will the CIO's decision to not select any of the vendors be trusted by the Board members?

- Employees were clamoring for the right to use their own mobile devices in the field for building bid estimates and securing sub-contractor quotes. The information security team had to decide which security configuration to adopt and where to lay the blame if the selected option proved inadequate against new attack vectors being used against mobile devices.

In each of the preceding instances, the leader must make a decision on which option to trust. Yet each decision is itself being evaluated as to whether the decision will earn the continued trust of others.

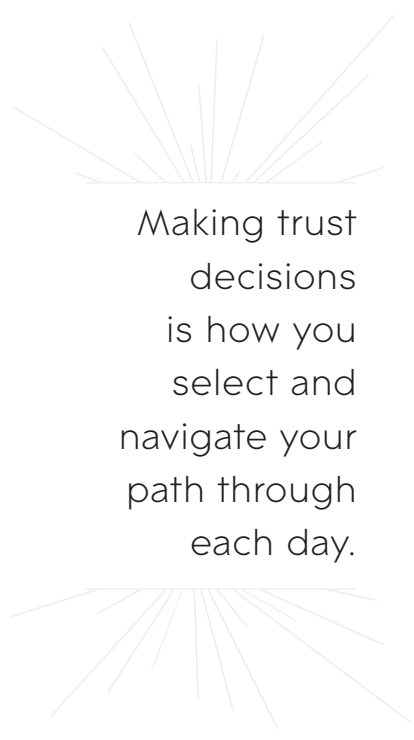
Deciding to trust is something you do every day. Frequently. Constantly. In business, your success or failure is measured by the decisions you make to trust your business partners, suppliers,

customers, market data, sales analyses, lab reports, and new-hire prospects. In daily life, you make decisions to trust people, objects, tools, systems, vehicles, computers, information, clothing, highways, stoplights, aircraft, entertainment media—even the water you drink and use to wash yourself.

Making trust decisions is how you select and navigate your path through each day. When you are more than one, acting as a part of a company, a community, a trading network, a social club, or a neighborhood gang, your trust decisions are even more critical. Your decisions have an influence on the collective; your success and failure often ride on whether the members of that collective place their trust in you and your decisions.

Will the Board vote to support your five year strategic plan? Will your team work overtime under your leadership to finish a new product ahead of schedule? Should we take your advice and buy added raw inventory? Have you double-checked all the financials for the proposed acquisition? Will they follow you over the bridge into enemy fire? These are all moments when you are being measured and evaluated on whether you—and your decisions—can be trusted.

What is trust? When does trust engage with our behaviors and our actions? How does trust govern our conduct in the many roles we perform? How do we decide to trust—as individuals, family members, employees, town citizens, consumers, corporate presidents and investors, bankers and borrowers, artists and concert goers, care givers and patients? How can you, individually and as part of the communities to which you belong, make better trust decisions? How can you become more trusted as a leader, manager, innovator, and advocate?



Making trust
decisions
is how you
select and
navigate your
path through
each day.

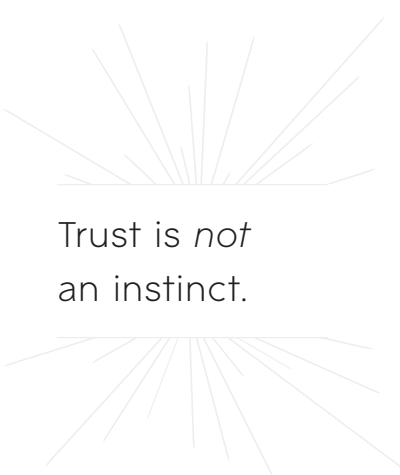
How can you better avoid placing your trust in people, objects, or things that are, in fact, untrustworthy? How can we design products and services that earn the trust of customers and others more rapidly, and sustain and increase their trust? How do we govern ourselves to protect against those people, objects, or things that exploit and abuse our trust, causing pain, losses, damages, and harm?

Your decisions guide how you interact with the objects, people, and information that you touch, select, use, share, and interact. Your decisions also direct you around, away from, and in avoidance of those objects, people, and information that you determine cannot be trusted. Trust is fundamental to how we interact with the world. Yet there are two prevailing characterizations of trust that must be dismissed—they are both fundamentally inaccurate.

WHAT TRUST IS

Trust is *not* an instinct.

First, trust is *not* an instinct. Sure, most trust decisions in daily life occur within an instant, so fast that the decision may be functionally inseparable from the actions taken in reliance on the trust decision itself. You decide to trust the red stop light facing opposing traffic only as you continue into the intersection without braking. You evaluate an online website's security only as you are entering your credit card information to complete a last-minute gift purchase. You consider the safety of entering a dark room only as you take your first step across the threshold. You decide whether to trust the directions being given by the service station attendant only as you are asking for the directions themselves.



Trust is *not*
an instinct.

Other trust decisions, especially in business, can be far more time-intensive and deliberative. They can extend over minutes, hours, days, weeks, or even longer. The slower pace at which these decisions unfold expose careful, complex balancings and weightings of variable facts and figures, as well as aggressive dissections of our “gut instincts.” When more assets are at stake, when more lives are in play, when there are potentials for greater wealth and greater loss, the decisions are more deliberative.

Complexity makes trust decisions more visible. We can see with greater transparency the variables of rules, information, outcomes, and costs involved in our decisions. Creating and entering a joint venture, committing to a new production plant, hiring a key management team member, accepting a proposal to sell your business—these are all trust decisions and often incredibly challenging to align all the moving parts. No instincts are welcomed.

Trust is *not* an emotion.

Second, trust is *not* an emotion. Trust is not an amorphous, vaporous variable within the quality of the human heart impossible of more precise expression. While we often express our trust in the vocabulary of emotions and metaphors, something far more analytical occurs when trust is achieved or lost. We retreat to emotional expressions of the presence or absence of trust because it is so hard to express the authentic attributes of trust.

So, what *is* trust?

Trust is the affirmative output of a disciplined, analytical decision process that measures and scores the suitability of the next actions taken by you, your team, your business, or your community. Trust is the calculation of the probability of outcomes. In every



Trust is *not*
an emotion.

interaction with the world, you are identifying, measuring, and figuring out the likelihoods. When the results are positive, you move ahead, from here to there. When the results are negative, you rarely move ahead; you stay put or you find an alternate path.

In making personal trust decisions, you are choosing to rely upon some one, some thing, or some *information* with which to live the next experience of your life, to finish the tasks that await completion—illuminate the room at dawn, provide music in the shower, nourish your child, transport yourself to work, read electronic mail, reply to electronic mail, attend a lecture, or select a teammate for a pick-up game of football. In every interaction, you make a trust decision that precedes what is next. You even ask if you can trust yourself! Am I strong enough, smart enough, or capable of doing what lays ahead? It is what we do as human beings—it is what most sentient species do as they engage with the world around them.

In making trust decisions within companies, networks, organizations, or communities, whether acting alone or as a collective, the process tracks to how you act individually. Tasks or objectives are defined, the available resources are evaluated, the possible results and risks are evaluated, and trust decisions are made as to how to proceed. Which option can be most trusted to achieve the intended outcomes? Which options present risks to our assets, our operations, or ourselves? Which information gives us the best analysis on which to make our decisions? Which tools can be most trusted to enable us to create new wealth?

Trust decisions are the most complex computations possible. Yet trust decisions have consistency, design, and structure that are possible to visualize and express with remarkable congruity, regardless of the complexity of the variables or the time during

which a trust decision must be completed. Trust decisions, properly executed, take account of the circumstances in which you are about to act; the qualities of the person, thing, or information on which you intend to rely; and the value you intend to invest, and realize, from giving your trust.

THREE ESSENTIAL QUALITIES OF TRUST

Trust, and the trust decision process, are governed by three qualities central to the analysis presented in this book. First, trust is a rules-based exercise. To complete trust decisions, you assemble and organize the rules that will direct your choices. As the trust decision process proceeds, you may discard some rules, determine that other rules cannot be met, or call up new rules that will be the foundation on which you move forward. But the fact remains—trust decisions are grounded upon, and executed against, a structured set of rules that define the boundaries and the outcome of each trust decision.

Second, trust decisions are fueled by information. As your rules are assembled, you seek information that allows you to calculate if the target of your decision (that is, the thing you are deciding whether or not you can trust) meets those rules. You sweep up information from your own memory, surrounding circumstances, records and reports, and reliable sources. You align the information against the rules and you calculate the results. Does the information about the target conform to your rules? If the information does not conform, or information required by the rules is not considered, then there can be no affirmative trust.

Third, trust decisions are mathematical. In order to align the information we gather with the rules we have assembled, we

deconstruct the rules and the information down to essential elements that enable simple calculations. For each rule, we ask: “Does the information meet the rule?” The deconstruction continues until the answer becomes a simple “Yes” or “No.” In order to trust some one or some thing, you add things up to determine if all of the elements are present under your rules. You make deductions that subtract from your analysis. Sometimes the deductions can outweigh everything else and you elect to not give your trust. At times, a single deduction (such as how you calculate the risk of death resulting from your decision) can be determinative.

In calculating trust, each of us also makes mistakes. Sometimes you will fire your engines and make decisions without enough information, or with information that later proves itself to be untrustworthy. You may rely on someone to help you make your decisions or rely on their opinion, only to discover that person was not a good choice. Through our mistakes, we refine how we calculate trust and update and revise our trust decision process, make new rules, and change what elements to take into account and how to measure them.

The results are remarkably binary—either there is an affirmative outcome or not, “yes” or “no”; “1” or “0.” “Maybe” is not allowed. Of course, as variables increase in number, the rules become more complex, the information greater in volume, the amounts at stake more valued, and the calculations are more difficult to execute. But, in all trust decisions, what is occurring is nothing more than a mathematical calculation. Do the results add up to trust?

These three qualities of trust decisions—rules-based; fueled by information; mathematical—allow us to embrace an understanding of trust that rejects both instincts and emotions. Instead, trust (or

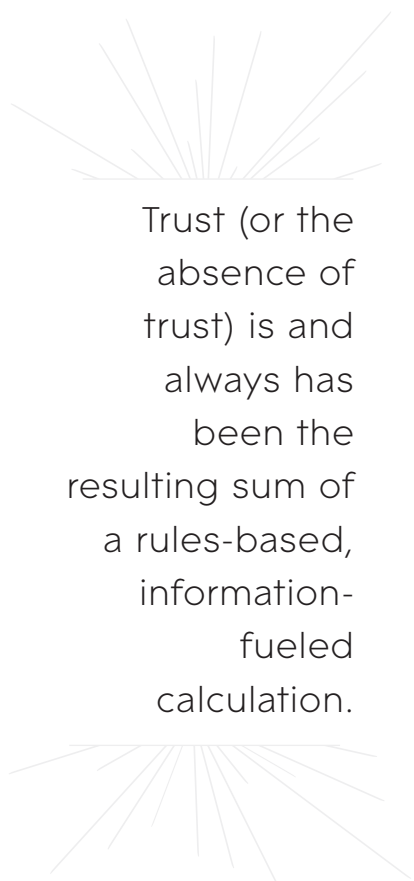
the absence of trust) is and always has been the resulting sum of a rules-based, information-fueled calculation.

In a digital world where we are struggling to sustain and build trust across a global, wired landscape of human affairs characterized by reports and allegations of cyberwars, digital theft, electronic espionage, and the loss of human dignity through ubiquitous surveillance, this essential truth changes everything.

FINDING YOUR WAY TO TRUST

Like any calculation, trust decisions have structure, sequence, and process. There is a beginning, a middle, and an end. At any level of society or commerce, there is remarkable consistency in how good trust decisions are made. Indeed, regardless of the complexity confronted in making trust decisions, for trust to exist, and for trust to be strong, the process must be executed rigorously. The rules must be followed; the required information must be collected; and the calculations must be completed. There are no shortcuts.

To succeed, a good map is needed, one that shows how the trust decision process unfolds from beginning to end. In the next chapter, you will be introduced to a new map for trust decisions. Unlike the old, paper maps in your car (or your parents' car), this one has layers that build one upon another until we can see the full picture of the trust decision process. At the same time, trust decisions are occurring in a sequence, moving from beginning to end. So, to explore this map, we will look down through the layers while also moving from a starting point to the end. It is a lot like watching a film and the process aligns well to how animated films once were created.



Trust (or the absence of trust) is and always has been the resulting sum of a rules-based, information-fueled calculation.

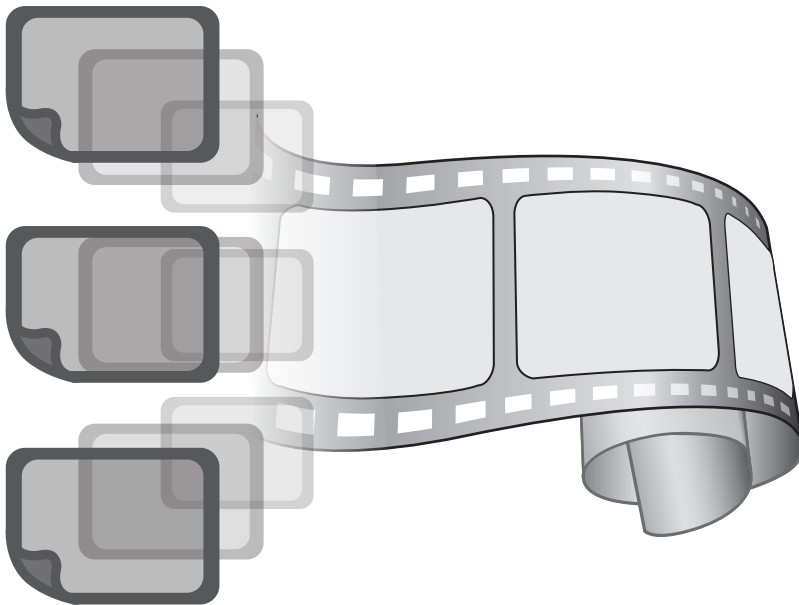
Films are, of course, a series of photographs presented at a high rate of speed that convinces the human eye of continuous action. In 2015, films are created and displayed at variable rates, 24 to 300 frames per second. The film technology controls how many frames are exposed during each second of action occurring before the camera. When we slow a film down, the differences between each frame become visible. When we focus on a particular element, such as the placement of a receiver's toes on a sideline pass, the changes between two or more frames are isolated. We can see the movement by seeing the differences between the images that become visible at each point in time. We can see what changes.

A trust decision is no different—*except that it is invisible. It happens in our minds.* The process is a continuing blur of dynamic, volatile calculations that often occur with impressive velocity and always involve complexity. A single trust decision is actually a series of decisions linked together, in which the shifting activity of all of the moving elements, actors, and variables becomes difficult to navigate. Your ability to stay focused on just one motion is challenged by the surrounding dependencies, interactions, counteractions, and entrances and exits from the boundaries of the images. But when we slow down the speed to freeze each moment as an individual frame for review, the trust decision process becomes more visible. Each element can be isolated better and, between two or more images, we can see what changes.

Of course, even if each frame of just one second of film represented one point in a trust decision, we would not have enough frames in that one second to display the full trust decision making process. To do so would require even more than 300 frames per second. Indeed, with automated trading systems and banner ad auctions

now measuring their velocity toward completion in nanoseconds (one billionth of one second), we would need quite a few more frames per second to devote one frame to each movement of change among all of the elements. But I believe the metaphor works—by using a freeze-frame analysis, we can stop the action and look more carefully at what occurs when you, your business colleague, your leader, or your team make trust decisions. We also need to see the layers of action within each frame.

Before computer animation, artists would paint and color individual illustrations on sheets of transparent celluloid (known as “cels”), with each character and each part of the scenery separately painted on those individual sheets. Then the cels would be stacked together and the camera would photograph the entire pile. The result would be a single, unified image of all of the individual sheets, creating one frame of film.



In the same manner, over the next several chapters, each layer of the trust decision process will be presented and explored in detail. As we begin to stack the layers one upon the other, and one frame proceeds to the next, you will be able to visualize the fascinating interactions that occur within and among the layers.

In every trust decision, there is always a controlling actor, the one making the final decision whether or not to trust. As our map unfolds toward the final destination, you will come to understand how the person deciding to trust interacts with the different layers and elements. You also will learn how those interactions are viewed by those who are evaluating the quality of the decision. When you are the person controlling that decision, improving your navigation skills across those interactions will help increase others' trust in your decisions.

So, let us take a look at our map, the Trust Decision Model.

THE TRUST VOCABULARY

In this chapter, you will learn the following words:

Chaining

Decision Maker (DM)

Information

Resources

Rewind and Recalculate (R & R)

Rules

Trust Decision Model

Trust Decision Target (TDT)

Work



CHAPTER 3


THE TRUST DECISION MODEL FROM 40,000 FEET

FOR EVERYONE ELSE in Wise Industries, a normal long, holiday weekend unfolded. But the CIO had a different few days. Restless nights, pre-dawn reviews of the strategic plans on her laptop, 17 phone calls to her team leads to double-check their field audits on the data centers and service providers, and three text messages from the chair of the Audit Committee: “What is your decision? Can we achieve \$47.5 million in savings by moving IT to the Cloud?” No matter that it was the weekend; at 09:00 AM tomorrow, she would be standing before the Committee.

Regardless of the size of your business, you likely have had one of those weekends sweating bullets with a deadline ticking toward you. A decision is required. It is a big one. The stakeholders above you will be ready to pounce on your decision, protecting their backsides by testing whether they can trust your analysis. Your team members are waiting to trust you, their leader, to make the decision that justifies the weekend’s phone calls and months of

advance field work. The bidding contractors and service providers are waiting for you to trust one of them and write a check that will make the winner a bit wealthier.

As you stand on the ledge, every aspect of your decision is reviewed again. And then, ignoring the fourth insistent text message, you pull up the five-year, return-on-investment projection on your laptop. Something catches your eye and your stomach turns. A cell is just not computing properly. A click reveals a key formula is missing a variable. You suddenly realize you never received the second audit to confirm the projected direct costs on which all the calculations depend.



Despite the apparent complexity, the good news is that trust decisions inherently follow a consistent, dynamic process. That process is the *Trust Decision Model*.

In this scene, I tricked you—you are the CIO! How do you make the decision? Do you freeze the process until you get the validation audit? Do you hope no one stands up and points out that the second audit was never initiated because the required funds had not been allocated? Who can you trust? What information can you trust to be real? Can *you* be trusted? What do your decisions look like? For each decision, what are you deciding to trust? If you have multiple options, how will your decisions influence how the final recommendation will be selected?

Navigating the answers to these questions is what makes decisions so challenging! Despite the apparent complexity, the good news is that trust decisions inherently follow a consistent, dynamic process which enables the decision to manage multiple, moving, and interactive parts. That process is the *Trust Decision Model*.

THE TRUST DECISION MODEL

This chapter introduces you to the Trust Decision Model from high above, as if you were flying 40,000 feet above the Earth. At that

altitude you can nearly see to the horizons of entire continents, but you cannot see the chaos and collisions of commerce and life below. This chapter is similar, providing you the full picture of the trust decision process. As the book proceeds, we will zoom in to see up close the complexity and remarkable structure of trust decisions and all of its variables and dynamics.

Professional cartographers emphasize that one of the hardest tasks in creating a map is determining what details to leave out. The same axiom plays out in this chapter. Not all of the moving parts of the trust decision, and not every variable in every calculation, can be displayed here. The Model displays trust decisions as a connected set of five layers; it is a visual map of the process. We will look at each layer and then end this chapter considering the full Model. In the following chapters of Part I, we will dismantle the layers in detail, much as an automotive racing team takes apart a race car piece by piece before rebuilding it in order to find greater speed.

TRUST DECISION CHAINING

As illustrated by our CIO's decision crisis, deciding to trust is not a single action but multiple decisions occurring in sequence. They connect, with each new decision leveraging the outcomes of prior decisions and then inputting and processing new variables that influence how the trust decision process progresses. The outcome of each decision links to the next, delivering information that the next decision requires. These multiple decisions within the trust decision process are visually expressed in the Trust Decision Model in this manner:



Moving from the left, each decision builds upon the previous one, overlapping much as the links of a chain. This introduces us to the Trust Vocabulary. In that vocabulary, these trust decisions are *chaining* together. No single decision is autonomous; each decision, if improperly executed, can dramatically change the direction of what follows. Indeed, some single decisions carry so much momentum across the process that an improper calculation can abort everything that follows, much like a space launch that is stopped even before it begins.

Chaining begins immediately, in the very first frame of the film of any trust decision. But the act of chaining is not entirely linear. In fact, if you were to slide the circles above into a stack, like the cels of an animated film, you would have a better sense of what is happening in every frame, with multiple decisions occurring concurrently in different layers of each frame. Decisions can also chain to multiple other decisions, whether within other layers in the same frame or in succeeding frames. Finally, as trust calculations progress, the results of later calculations often direct the decision process to rewind, refine the input to previous linked decisions, recalculate the decision, and then move forward again (“Three links back, now one link forward again, and the next . . .”). In our trust vocabulary, this is called *Rewind and Recalculate (R & R)*.

The result is similar to an athletic coach watching film of a game, rewinding and stopping the action to identify all the variables required for better decisions in future games. That is likely no different from just about any analysis you are asked to make in business (or in life)—moving in one direction, making sequential decisions, learning new data, and going back to reevaluate earlier calls, ideally before any harm comes from making decisions

without the new data. There is one important difference between coaches in the film room and trust decisions in business and in life—you must make your trust decisions in real time, with a clock always ticking.

SPECIFYING THE WORK

Every trust decision is a determination to trust an object, person, group, system, device, or information asset to be used to accomplish a specific task:

- What do you wish to accomplish?
- What must your team do in order to succeed?
- How many widgets per hour need to be constructed?
- What information must be acquired or produced?
- How will performance of these tasks be measured?
- How will success be defined? What will represent failure?

In asking these types of questions, you are building a specification. In our trust vocabulary, this specification is called *Work*. It can be very simple, such as hammering a nail into a wall or composing a quick email to your supervisor to report on the day's events. Work also can be amazingly complex, such as deciding to move the IT operations to the Cloud. In later chapters, we will explore the full complexity of how to develop the specification for Work. For now, to understand the Model, it is sufficient to think of Work as the job that needs to get done. In many ways, Work is no more difficult to understand than that.

FINDING THE TARGET

Each trust decision, informed by a specification of Work, is focusing on and evaluating a target—a tool, system, device, information, or other resources—to determine whether or not it can be trusted to complete the Work. The target is the end point of each trust decision; in our trust vocabulary, it is a *Trust Decision Target* (or *TDT*). Each decision is being made by the CIO, a Board, your team, or you; in our trust vocabulary, the entity making the trust decision is called the *Decision Maker* (*DM*).

A TDT is always a resource that the DM evaluates to use in performing the Work. In our trust vocabulary, the overall universe of assets from which TDTs may be selected or assembled is called *Resources*. A TDT can take many forms. It can be:

- a strategic business partner or team member, selected to complement your company's strengths to create greater market share and revenue.
- a person, such as a teacher to be trusted as a source of knowledge and training skills for your child.
- a group, such as the members of a pick-up game of football in the schoolyard.
- a tool, whether it is a hammer, a computer program, or a residential home.
- a system, such as a retail clothing warehouse storage and conveyor system, a distributed, connected system of data centers, or a Cloud-connected wristwatch.

» a book, a magazine, a poem, a database, a purchase order, or a web page of digital content.

» yourself.

» Can you trust your own strength to lift a heavy box of books, your ability to calculate in your head the estimated harvest yield for the season, or your judgment in making a decision to spend \$47.5 million one way or another without any due diligence or consultations with others?

» Can others trust you to make effective decisions about the direction of the company's marketing campaign? Do you make good choices in hiring new members of the team? Have you properly analyzed the capabilities of a proposed joint venture to create new wealth for the company's shareholders?

Not every trust decision for a specific TDT has a favorable result. On any day in your ordinary life, you make decisions that a TDT is not trustworthy. The summary sales report for the Southeast region does not have enough detail to produce a new quarterly revenue projection for each store location. A potential team member seems not to have the “right” answers to questions you ask regarding career ambitions and dreams. Your partner's three-inch dress shoe heel was a possible hammer for nailing up that one picture, until you remember the drywall was mounted on concrete. In each case, you completed the trust decision process and determined the TDT was not to be trusted to perform the Work.

The same structural process unfolds when evaluating the utility of digital assets as TDTs. Networks, systems, devices, applications, information assets—their digital quality does not alter how any of us is wired to calculate whether to trust. With each possible use of a digital asset, an affirmative determination must be calculated that a specific TDT can be useful in completing the Work.

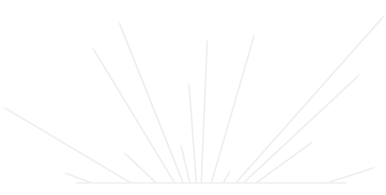
THREE OPTIONS IN EVERY TRUST DECISION

If every trust decision focuses on a specific TDT, how does the DM locate and select the target itself? As the CIO, how would you define the boundaries around the various contractors, systems, devices, applications, and data sources in order to construct what the TDT looks like? What are your options?


At every level, and in each frame, a DM is constantly evaluating and comparing among three options for completing the Work:

- Do nothing.
- Undertake the Work using entirely one's own personal capabilities: physical strength, agility, counting on your fingers and toes—whatever it takes without using any other Resources.
- Select one or more external Resources to be trusted as a TDT with which to complete the Work.

The process is a dynamic one. Very rarely will the first option make sense—after all, performing Work produces income, creates product, advances knowledge, or delivers entertainment. Nor does the second option frequently stand up as an option—in business,



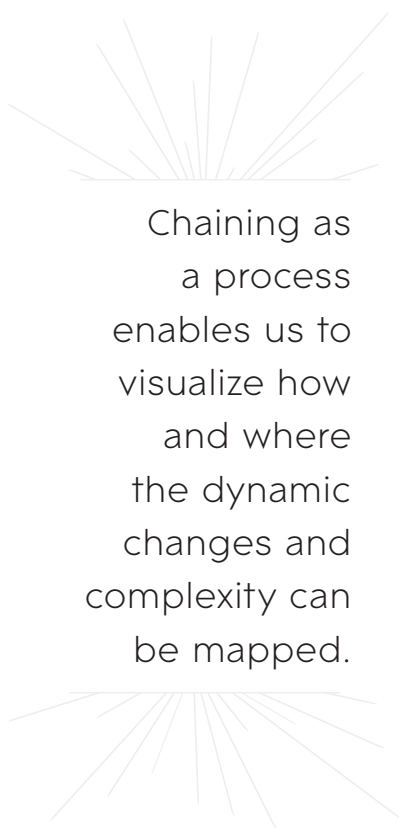
A DM is constantly evaluating and comparing among three options for completing the Work.



teams, or communities, we maximize our productivity by working with others and using others' Resources, not ignoring them. But exercising the third option to select any Resource or Resources to be a TDT requires a predicate decision—is the selection a viable choice? If not, additional decisions chain together, more information is acquired, and the requirements for what will be suitable Resources refine until, at some point, the process identifies a specific Resource (or combination of Resources) to be worthy of further evaluation. The identified Resource(s) become the TDT, literally the target for the trust decision—can the Resource(s) be trusted to perform the Work?

Making any decision that can be trusted is made more complicated by the reality that the variables to be considered are volatile, constantly changing. Surrounding conditions may shift, Resources may alter in their condition or availability, or a customer's requirements may be revised. The DM must be capable of identifying and responding to the changes if the resulting decisions are going to be trusted. Every trust decision is comparable to how a surgeon once described his work to me, "We do the same thing as an auto mechanic, except the engine is still running at all times."

Chaining as a process enables us to visualize how and where the dynamic changes and complexity can be mapped, and the interactions among all of the moving parts can be recalculated toward measuring the trustworthiness of a TDT. But one constant, from beginning to end, is that Resources are the inventory from which TDTs are selected, evaluated, and used. So the Trust Decision Model shows Resources as the top layer:



Chaining as
a process
enables us to
visualize how
and where
the dynamic
changes and
complexity can
be mapped.

RESOURCES



Resources have immense diversity—people, objects, systems, information, money, or property. But a Resource (and any TDT) is always an identifiable object, some one or some thing, physical or digital, that you can identify, classify, and ultimately evaluate, individually and as part of a collection or assembly with other Resources, for its trustworthiness.

RULES

Since trust decisions are rules-based, rules are an inherent, continuous presence in the process. Rules do one of three things: they express what is required, what is permitted, or what is prohibited. In our trust vocabulary, all of these are *Rules*. The Model presents them as a foundational layer below the decision chaining:

RESOURCES



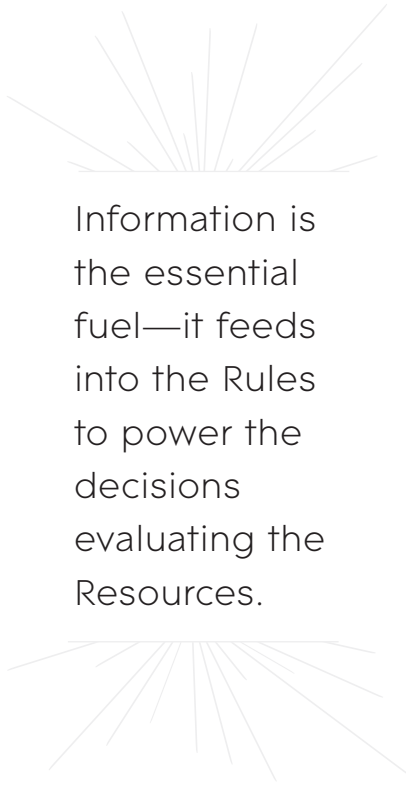
RULES

Rules drive every aspect of every trust decision. Our Rules shape the selection of possible Resources to consider or reject, the structure and mathematics of our calculations, and the probabilities the DM requires for a final trust decision to result. Decisions at each layer of each frame test the adequacy of Rules, mandate the Rules to be selected, and instruct the authorship of new Rules upon which you may rely in making future trust decisions.

There are many sources of Rules—formal laws and regulations, guidances and interpretations, corporate policies and procedures, contractual obligations and informal rules of engagement, best practices, technology standards, and code-specific architectural requirements, to name just a few! For IT architects, business executives, compliance officers, venture capitalists, or Scouting leaders, the daily challenge in decision making is to identify and properly navigate the Rules. Once the Rules are known, everything else follows. Later chapters introduce new ways of thinking about those processes and how to identify, filter, rank, author, revise, and execute with greater precision the Rules that matter. For now, at 40,000 feet, it is enough to know they are the foundation for the entirety of the trust decision process.

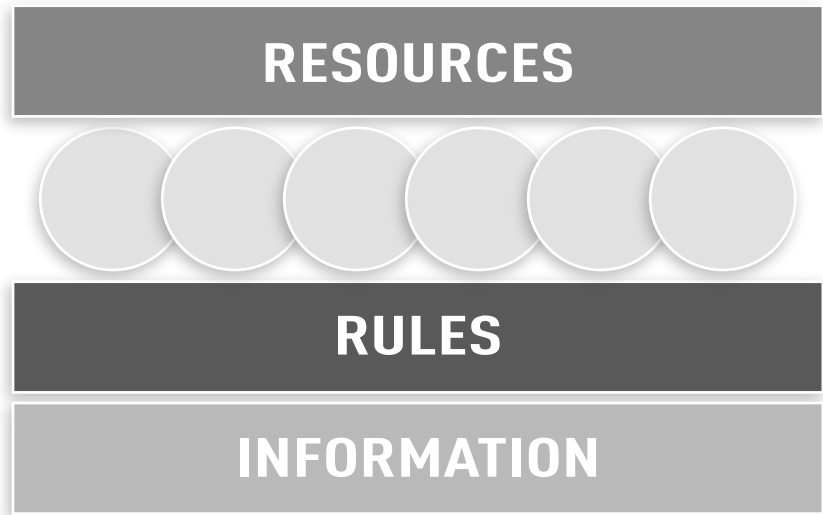
INFORMATION

To execute, follow, author, apply, or make trust decisions based on Rules requires information (*Information*, in our trust vocabulary). As introduced in Chapter 2, Information is the fuel on which trust decisions proceed. The interactions among Rules and Information are continual and complex. Information is required about the Resources, the Work, and how success in performing the Work will be measured. Information about the surrounding circumstances, the intended results, the possible risks, and the potential rewards



Information is the essential fuel—it feeds into the Rules to power the decisions evaluating the Resources.

and losses—all of this knowledge is required to execute and chain together the layers and the frames into a complete trust decision. The interdependence among Information, Resources, Rules, and chained decisions is inherent. Information is the essential fuel—it feeds into the Rules to power the decisions evaluating the Resources. In reverse, evaluation of the Resources drives adjustments in the Rules, and new Rules require new Information. The Model shows the presence of Information in this manner:



TIME

In making decisions, time is the one most overlooked asset, yet it is the most valuable asset in play within every trust decision. You surely have felt the pressure to make a decision by a defined deadline. Whether it is a large or small one, the imposition of deadlines changes how a decision unfolds, compressing the time to make it into a confined space. In business, government, transit, education, home repairs—time often emerges as the variable that can most alter the decision process and the outcomes.

When time is compressed, we tend to make different choices

in identifying Resources, describing the Work, selecting Rules, acquiring Information, and Rewinding and Recalculating earlier chained decisions. While the chaining architecture of trust decisions works best when decisions chain vertically between layers and then across frames, the compression of time imposes a linear structure, forcing progress toward making a final decision. Deadlines reduce and quickly eliminate the ability to perform look-backs and revisions, making each decision downstream more reliant on the accuracy and effectiveness of those preceding it. Returning to this chapter's opening scenario, realizing the five-year, return-on-investment projection is defective, you, as CIO, no longer have the time to go back. The deadline is now. You are going to make your decision based on the weeks of preceding analysis. You feel the pressure to send the Audit Committee chair a text response, even though you have one more night to process the decision. It is Sunday night at 09:15 PM. What are the implications of the choice to be made?

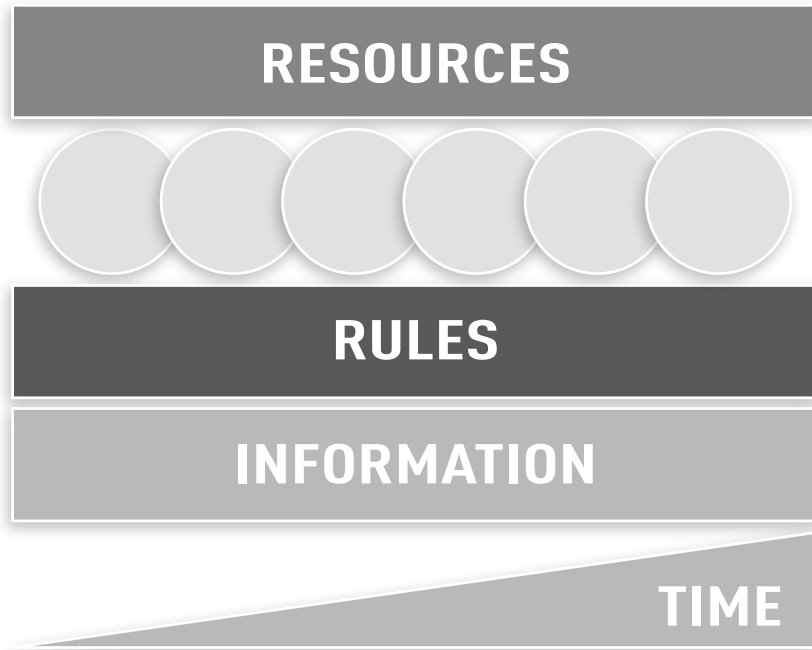
TIME IS MONEY—AND MAYBE A LOT OF MONEY

In the Trust Decision Model, two measures of time are initially important. The first measure is the time consumed by the trust decision process to reach a final decision. As mentioned in Chapter 2, while many trust decisions are nearly instantaneous, that is not always the case. When the decision is a “bet the company” decision, a significant amount of time may be consumed. In our daily affairs and in planning the big decisions, we rarely focus on that time metric or the accumulating cost of taking the time to make decisions that must be trusted. Executives, advisors, lawyers, department managers, compliance executives, consultants, accountants, line employees, service providers, contractors—in a major corporate deal, all are consuming time to work toward the ultimate decisions of a complex deal.

Despite this fact, in nearly 30 years of participating in corporate deals, I rarely saw a calculated estimate of the all-in time required to move through the trust decision process to reach a final determination. The estimates I did see were rough guesses, more focused on the out-of-pocket costs of doing the deal. Never did I see alternative process models that compared alternative strategies for how to complete the contributions of each stakeholder in less time. What tools would enable the work to be done more quickly? What process rules will better minimize the risk of overlooked validation studies? How can we leverage technology to enable faster analysis? At best, during those years there was an occasional comparison of raw costs, such as the rates charged for using outside versus inside counsel, or sending contract due diligence to India rather than Des Moines. Even now, we are just beginning to see project design tools that allow resource planning to consider alternative scenarios. The focus continues to be on financial costs, not on time.

The second measure of time important to trust is the time that is on the other side of the trust decision process—the lost opportunity cost of a decision delayed by the process. When you are making decisions in business, you are driven by the appetite to create new wealth or preserve existing wealth. When trust decisions consume time, they are also consuming the time on the other side of the transaction when wealth could be created or lost. As CIO, the projections show the company would save \$1.2 million in operating costs each month; if you decide to defer the decision for two more weeks while the second audit is performed, the delay in making the decision has a \$600,000 direct impact. Even in making personal decisions (when to have dinner, what movie to watch, or which lawn mower to purchase), time is the ultimate currency in play when making trust decisions.

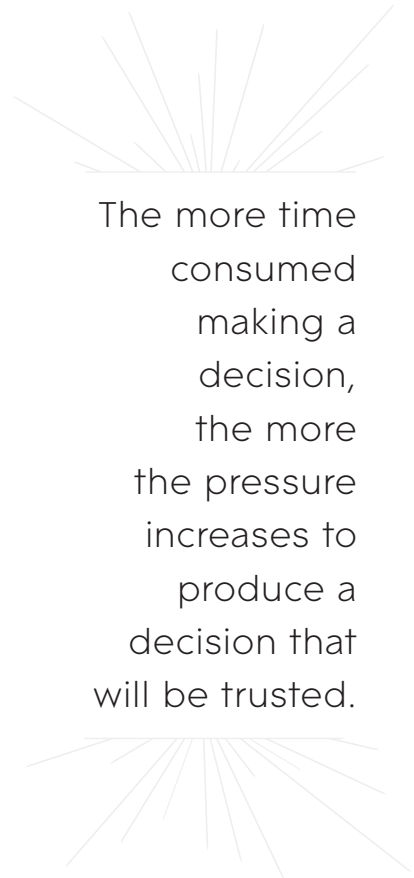
Both of these measures of time—the time consumed and the lost opportunity time—are important and can be incorporated into the Model in parallel:



As time advances from left to right, the time consumed by the decision (and the related costs) grows in volume. The opportunity value of time lost awaiting a decision (and the related wealth to be created or preserved) grows as well. Both measures are proportional; and the more time consumed making a decision, the more the pressure increases to produce a decision that will be trusted.

A FINAL GLANCE FROM 40,000 FEET

When a deadline is imposed, forcing linear structure onto the trust decision process, we must start making choices for which no further R & R will be possible: some Resources are not viable to further evaluate; some Rules will be ignored; or some Information will not



The more time consumed making a decision, the more the pressure increases to produce a decision that will be trusted.

be gathered or, if collected, may not be properly vetted. You surely have been there when the deadline is forcing a decision and you have to make choices. You know a Resource, a Rule, or Information may be relevant but, driven by the deadline, you knowingly exclude it from further consideration. Time has run out.

In contrast, when there are enormous assets on the line—a major sale, a joint venture, imposing a new regulation, filing a major lawsuit, expanding a division, reducing the workforce—you also want to make the best possible decisions. You want your decision to be trusted; you want to be trusted as contributing well to the decision. If there is no deadline, then the decision process expands, allowing the circling back and recalculations that are part of its architecture. More Resources are considered; more combinations of Resources are modeled; the outcomes under more Rules may be evaluated; new Information is sought against which to align the Rules; and existing Information is vetted more closely. You choose to be more thorough even while time ticks away.

PERSPECTIVE MAKES A VAST DIFFERENCE—DOESN'T IT?

By looking at the Trust Decision Model, even from a “higher elevation,” you can see what happens when those choices are occurring. Under deadlines, with big stakes on the line, or in ordinary decisions, you can tag each one of the choices you make in moving forward as a decision to leave out or add a Resource, a Rule, or Information. It is how you or any DM proceed in every decision. Exclusions are intended to save time (to make the deadline) in order to gain time (reducing the lost opportunity cost); additions consume more time (for a more thorough analysis) and potentially cost time (deferred opportunity) on the other side of the pending decision.

Yet, at 40,000 feet, we can observe what happens when elements are included or excluded. To make those decisions, the constituents within the layers must be ranked. Rules must be mathematically scored and stacked; Information must be scored and stacked; and Resources must be scored and stacked. How else do we express the importance or disposability of any specific element? The process is entirely mathematical. The Rules, Information, or Resources included or excluded from the later frames of the decision process result from a ranking of their values—the process is not emotional, it is arithmetic. Once the rankings are in place, we can draw lines and boundaries.

A more complete trust decision, however, has one additional critical measure to be introduced in this chapter: wealth. Decisions that are thorough—decisions that are to be trusted—create more wealth. When, within the trust decision, there is greater, more complete balancing among Resources, Rules, and Information, and the chaining of decisions is not forced by deadlines into a linear structure, the outcome will always be a decision that is more successful. Fewer elements are excluded—more Resources are considered; more Information is collected; and more Rules are evaluated—creating better measurements of the probabilities of achieving success in performing the Work. That is the ultimate measure of trust—achieving success consistent with the calculated probabilities.

Yes, more time is consumed and, in theory, that can mean a growth in lost opportunity cost. But imagine if a more thorough decision can be generated *and* given velocity, producing outcomes that are more trusted and require less time, thereby not incurring the greater lost opportunity cost. Imagine a more comprehensive consideration of the full portfolio of what the Trust Decision Model embraces, with

fewer exclusions of Rules, Information, and Resources that deadlines or competitive pressures would otherwise require.

A MODEL THAT MAKES YOU A BETTER LEADER

As someone whose decisions are to be trusted, is that not what you would like to report? As someone who evaluates the decisions of others (and we all do), would you not value greater thoroughness and velocity in the decisions you review? Of course. Had you, as CIO, previously built a Rule that did not allow projected direct costs to be input without your sign-off on the second audit report, there would be no stomach churning. Had your decision model forecasted the opportunity cost of delayed decisions, spending an extra \$50,000 to accelerate the second audit would have been viewed as a small added expense to achieve a faster, more trusted decision.

In its basic layout, the Trust Decision Model enables us to begin seeing our decisions structurally, as a dynamic of known, identifiable moving parts within a chaining of decisions. We begin to understand, against the measure and value of time, how our decisions to exclude or include any of the moving parts, arithmetically calculated and marked by drawn lines, affect the trustworthiness of our decisions. As the Trust Decision Model further unfolds, and we look ever closer at further layers and frames, the importance of connecting trust and time becomes essential, determining who will win or lose in the next generations of the Digital Age.

ZOOMING IN FOR A CLOSER LOOK

In the next chapter, we will zoom in to look closely at the first layers of the first frame and how we conceive and stack those

layers. Indeed, since so much is going on in the first moments of a trust decision, imagine we are increasing our film speed from 24 to 1,000 frames per second. By increasing the number of frames, we are creating 1,000 pictures of what occurs within one second. Now comparisons between the frames will expose the very small, but important, shifts at each layer and the interactions among the moving parts will become more visible.

One more thing: remember how trust decisions are occurring inside our minds? As we move ahead, we are going to be looking inside, as if the exterior of our trust decisions became transparent. As that level of detail comes into focus, moving slowly frame by frame, you soon will discover that many trust decisions are aborted before they truly begin. “Taking the risk” means choosing not to calculate trust and the first opportunity to do so occurs far earlier than you might ever imagine.

A Note from Jeffrey Ritter



Thank you for your interest in **Achieving Digital Trust: The New Rules for Business at the Speed of Light**. I hope you have enjoyed what you have read so far!

This book has many different audiences. If you don't feel it is right for you, please pass it along to those who might benefit from the insights, tools, and strategies presented across its pages.

I also welcome your reactions to what you have read—good or bad, favorable or unfavorable. Gaining momentum in the trust revolution will require your feedback and I look forward to hearing from you, whether or not you purchase the book! Just drop me an email at jeffrey@jeffreyritter.com.

You can purchase your copy of the book on Amazon [here](#), in paperback and Kindle formats.

The digital trust revolution has begun!

Again, my thanks.

A handwritten signature in black ink, consisting of two parts. The first part is a stylized 'J.R.' and the second part is a more complex, cursive signature that appears to be 'Jeffrey Ritter'.

AUTHENTIC • SECURE • CONTROLLED • RELIABLE • MEASURED • GOVERNED

**IN THE GLOBAL, ALWAYS-ON, DIGITAL MARKET,
THERE ARE NO MORE SECOND CHANCES IN
YOUR DECISION MAKING.**

**NO DECISION IN BUSINESS OR GOVERNMENT WILL BE MADE IN THE 21ST CENTURY
WITHOUT RELYING ON DIGITAL INFORMATION. IT MUST BE TRUSTED.**

For any leader or executive, the uncomfortable truth is our trust is under attack, making each decision more vulnerable. The same is true for our customers—without trust, they will shift their spending quickly to other options.

The challenge is not merely to restore trust. Instead, those who survive and prosper will be those who engineer and deliver digital trust.

Achieving Digital Trust presents to business executives, IT strategists, and innovation leaders something remarkable—a complete tool-kit of new strategies and resources that will change how they make decisions that matter, decisions that can be trusted.

Using the Trust Prism, the signature innovation introduced here, along with other tools to be discovered in this book:

- » **LEADERS WILL MAKE BETTER DECISIONS FASTER AND GAIN GREATER TRUST IN THEIR LEADERSHIP.**
- » **BUSINESS EXECUTIVES WILL BE ABLE TO VISUALIZE AND MANAGE THE COMPLEXITY OF THEIR COMPANY AND THE WIRED ECOSYSTEMS IN WHICH THEY COMPETE.**
- » **IT ARCHITECTS, LAWYERS, AUDITORS, AND COMPLIANCE EXPERTS CAN WORK TOGETHER, SPEAK THE SAME LANGUAGE, AND MEASURE SUCCESS RATHER THAN MANAGE RISK.**
- » **INFORMATION PROFESSIONALS CAN GAIN CONTROL OF DIGITAL INFORMATION AND ASSURE THAT AUTHENTIC, ACCURATE, AND RELIABLE KNOWLEDGE ASSETS FUEL THE NEXT CHAPTERS OF THE DIGITAL AGE.**

JEFFREY RITTER is the creator of: the Trust Decision Model, the Trust Vocabulary, the Rules for Composing Rules, the Unified Rules Model, the Unified Information Model, the Trust Prism, and the Velocity Principle—all presented in this book.

Recognized for his international leadership in shaping the legal rules for online commerce, he currently teaches graduate courses in information governance and privacy engineering at The University of Oxford and Johns Hopkins University. He has also taught at Georgetown University Law Center.

Visit www.jeffreyritter.com to learn more.

