IRA WINKLER AND DR. TRACY CELAYA BROWN

YOU CAN STOP STUPID

STOPPING LOSSES FROM ACCIDENTAL AND MALICIOUS ACTIONS

WILEY

You CAN Stop Stupid

You CAN Stop Stupid

Stopping Losses from Accidental and Malicious Actions

Ira Winkler
Dr. Tracy Celaya Brown

WILEY

You CAN Stop Stupid: Stopping Losses from Accidental and Malicious Actions

Published simultaneously in Canada

ISBN: 978-1-119-62198-0
ISBN: 978-1-119-62206-2 (ebk)
ISBN: 978-1-119-62204-8 (ebk)

Manufactured in the United States of America

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019956718

To my incredible wife, Adriana, who pushed me harder to write this book than I pushed myself. —Ira

To my extraordinary husband, Mel, and my wonderful family, I love and appreciate you more than words can ever express. —Tracy

About the Authors

Ira Winkler, CISSP, is president of Secure Mentem and author of *Advanced Persistent Security*. He is considered one of the world's most influential security professionals. Ira began his career at the National Security Agency (NSA), where he served in various roles as an intelligence and computer systems analyst. He has since served in other positions supporting the cybersecurity and risk management programs in organizations of all sizes. His specialty is the human aspects of technology and loss mitigation. He has received several lifetime achievement awards, including the CSO COMPASS Award, which dubbed him "The Awareness Crusader." Ira has written books and speaks around the world about cybersecurity, risk management, and the human aspects of security and technology. Ira can be reached through his website at `www.irawinkler.com`.

Dr. Tracy Celaya Brown, CISSP, is a sought-after IT and business consultant and the president of Go Consulting International. Clients consider her their "secret weapon" as she helps organizations define and implement their security strategy and develop a solid organizational culture of security. Committed to making the digital world more secure and influencing the next wave of IT and security professionals, she is also a facilitator, researcher, author, innovative leader, and an award-winning international speaker. Dr. Tracy Celaya Brown can be reached through her website at `DrTre.com`.

About the Technical Editors

Adam Shostack is a leading expert on threat modeling, and a consultant, entrepreneur, technologist, author, and game designer. He's a member of the BlackHat Review Board, and he helped create the CVE. He currently assists many organizations to improve their security via Shostack & Associates and advises startups, including as a Mach37 Star Mentor. While at Microsoft, he drove the Autorun fix into Windows Update, was the lead designer of the SDL Threat Modeling Tool v3, and created the *Elevation of Privilege* game. Adam is the author of *Threat Modeling: Designing for Security* and the co-author of *The New School of Information Security.*

Dr. Lance Hayden has 30 years of experience in the information security field, a career that includes roles in industry, government, and academia. He is the chief information security strategist for Vericast, as well as a professor at the University of Texas School of Information. Dr. Hayden's research and expertise includes understanding information security awareness and behavior, and he is the author of *People-Centric Security: Transforming Your Enterprise Security Culture.*

Acknowledgments

A book like this represents the experiences and lessons learned throughout our entire careers. As such, we owe a debt of gratitude to many people, some of whom we've lost touch with. So to all of you, the best we can do is send you good karma and hope we have somehow returned the favor. There are, however, a few people to whom we need to truly express our thanks.

First is Jim Minatel, who worked with us to determine the book we really wanted to write and allowed us to share our passion and experiences with you, the reader. We also owe an immense debt of gratitude to Kelly Talbot, our development editor, who kept us from sounding stupid and helped us get our points across. During the review process, we cringed every time we saw comments from Lance Hayden and Adam Shostack, our technical editors. The cringes were due to the fact that we knew that each of their comments were well thought out, would add immensely to the quality of the book, and would require us to do a lot of research and hours of more writing. They both have an incredible breadth and depth of experience in the field and truly know how to incorporate research into practice. If you find value in this book, it is as much a credit to them as it is to us. Dr. Nicklas Dahlstrom of Emirates also provided incredibly valuable guidance in forming our thoughts on the integration of safety science with mitigating user-initiated loss. We likewise owe a massive thanks to Adriana Winkler, who read everything to ensure that it made sense to laypersons as well as to the technical experts. We also want to give a special thanks to Rupin Kotecha of Digital Guru, who was the catalyst for putting us in contact with Jim Minatel to get this book started. Finally, we need to thank Britta Glade of RSA Conference, who was the instigator for our working together.

—Ira Winkler and Dr. Tracy Celaya Brown

Foreword

So, here it is, in your hands. A book with a message that took the field of cybersecurity only a couple of years—decades at most—to come around to. Its premise is something that human factors professionals wish they could get through to the people they work with every day: the medical device manufacturers, the cockpit designers, the "autonomous" vehicle developers, the construction site planners, the procedure writers—if they could just get this simple message. Spoiler alert, this is the message: If your people are doing stupid things, it's not because you have stupid people. It's because you have a stupid system.

And then to think that human factors is a field that's been around for almost 80 years. It was at the basis of the discoveries that led to this premise. Design a cockpit that puts two toggle switches next to each other—one for the landing gear, and the other for the flaps—and you are going to get belly landings. Which the new, bigger, badder Boeing B-17 bomber was getting a lot of during WWII. The solution was not punishing the errant pilots. It wasn't putting up posters exhorting them to try harder. It wasn't mounting an incident counter on the wall that announced how many days had gone by without a fellow B-17 pilot planting the aircraft on its belly. As long as the toggle switches were inviting pilots to mix them up, then pilots would mix them up.

In 1943, Alphonse Chapanis, a human factors pioneer, fashioned a little flap handle and a little wheel in a workshop and mounted them on the respective toggle switches of some of the B-17s. The ones that were thus equipped never belly-landed again. A gear lever that looks and feels like a wheel, and a flap handle that looks and feels like a flap, now constitute a design and certification requirement for airplane cockpits. If your people are doing stupid things, then you have a stupid system. So, go fix your system. As Ira and Tracy put it, "The simple fact is that a user can't initiate loss unless an organization creates an environment that puts them in a position to do so."

When you suffer a loss, it is, of course, attractive to gravitate to emotionally satisfying and low-cost interventions. Blame the person who messed things up. Hold them accountable. But Ira and Tracy have a different, and more sustainable, message for you. If you want to talk about accountability, then *you* are actually accountable for setting your people, your users, up for success. *You* are accountable for avoiding safety barriers that get unreasonably in the way of work, which leads to undesired side effects. *You* are accountable for showing nonjudgmental curiosity in how work actually gets done, rather than how you, or your designers, imagined it to be done. *You* are accountable for giving your people error-resistant and error-tolerant designs to work with. *You* are accountable for reducing the resource constraints and goal conflicts that set your system up for drifting into failure. *You* are accountable for valuing your people's native resilience and adaptive capacity over dogmatic, strict rule-following. And *you* are accountable for identifying and enhancing the capacities in your people that make things go well.

There is so much you can do to stop "stupid." But you need to see "stupid," not as the root cause of your problems. If you discover "stupid" somewhere, then that is just the beginning of your inquiry, of your curiosity, of your journey toward improvement. "Stupid" comes from somewhere. It is an effect, an outcome—not a cause. When you start looking behind that label "stupid," you will find lots of things that actually make sense: where people were looking at the time, which things they considered important to focus on, what knowledge they brought to bear, which interacting goals they were trying to achieve simultaneously, what resource constraints they were trying to make up for, what work they were trying to get done despite all the obstacles you may well have helped put in their way.

If you think your people were doing "stupid" things, then muster the courage to go behind that label and face up to what you find. Stop stupid by fixing your system. Because otherwise the label "stupid" might well stop with you, and stick.

Sidney Dekker

Professor, Griffith University (Australia)

and Delft University of Technology (Netherlands)

Contents at a Glance

Contents

Introduction

We believe that the title of a book is perhaps its most critical characteristic. We acknowledge that the title, *You Can Stop Stupid* is controversial. We had considered other possible titles, such as Stopping Human Attacks, but such a title does not convey the essence of this book. Although we do intend to stop attacks that target your users, the same methodology will stop attacks by malicious insiders, as well as accidents.

The underlying problem is not that users are the targets of attacks or that they accidentally or maliciously create damage, but that users have the ability to make decisions or take actions that inevitably lead to damage.

That is the fundamental issue this book addresses, and it makes a critical distinction: The problem lies not necessarily in the user, but also in the environment surrounding the people performing operational functions.

What Is Stupid?

Managers, security specialists, IT staff, and other professionals often complain that employees, customers, and users are stupid. But what is "stupid"? The definition of "stupid" is having or showing a great lack of intelligence or common sense.

First, let's examine the attribute of showing a great lack of intelligence. When your organization hires and reviews people, you generally assess whether they have the requisite intelligence to perform the required duties. If you did hire or retain an employee knowing that they lacked the necessary intelligence to do the job, who is actually stupid in this scenario: the employee or the employer?

Regarding a person who shows a great lack of common sense, there is a critical psychological principle regarding common sense: You cannot have common sense without common knowledge. Therefore, someone who is stupid for demonstrating a great lack of common sense is likely suffering from a lack of common knowledge. Who is responsible for ensuring that the person has such common knowledge? That responsibility belongs to the people who place or retain people in positions within the organization.

In general, don't accuse someone in your organization of being stupid. Instead, identify and adjust your own failings in bad employment or training practices, as well as the processes and technologies that enable the "stupidity."

Do You Create Stupidity?

When people talk about employee, customer, and other user stupidity, they are often thinking of the actions those users take that cause damage to your organization. In this book, we refer to that as *user-initiated loss* (*UIL*). The simple fact is that a user can't initiate loss unless an organization creates an environment that puts them in a position to do so. While organizations do have to empower employees, customers, and other users to perform their tasks, in most environments, there is little thought paid to proactively reducing UIL.

It is expected that users will make mistakes, fall for tricks, or purposefully intend to cause damage. An organization needs to consider this in its specification of business practices and technological environments to reduce the potential for user-initiated loss.

Even if you reduce the likelihood for people to cause harm, you cannot eliminate all possibilities. There is no such thing as perfect security, so it is folly to rely completely on prevention. For that reason, wise organizations also embed controls to detect and reduce damage throughout their business processes.

How Smart Organizations Become Smart

Consider that large retail stores, such as Target, have a great deal to lose from a physical standpoint. Goods can be physically stolen. Cashiers can potentially steal money. These are just a couple of common forms of loss in retail environments.

To account for the theft of goods, extensive security controls are in place. Cameras monitor areas where goods are delivered, stored, and sold. Strict inventory control systems track everything. Store associates are rewarded for reporting potential shoplifters. Security guards, sometimes undercover, patrol the store. High-value goods are outfitted with sensors, and sensor readers are stationed at the exits.