"Endlessly fascinating, brimming with insight, and more fun than a book about failure has any right to be."
—Charles Duhigg, author of *The Power of Habit*

MELTDOWN

What PLANE CRASHES, OIL SPILLS, and DUMB BUSINESS DECISIONS Can Teach Us About How to Succeed at Work and at Home

CHRIS CLEARFIELD and ANDRÁS TILCSIK

Prologue

A DAY LIKE ANY OTHER

"It was the quotation marks around
'empty' that got me."

I.

It was a warm Monday in late June, just before rush hour. Ann and David Wherley boarded the first car of Metro Train 112, bound for Washington, DC, on their way home from an orientation for hospital volunteers. A young woman gave up her seat near the front of the car, and the Wherleys sat together, inseparable as they had been since high school. David, sixty-two, had retired recently, and the couple was looking forward to their fortieth wedding anniversary and a trip to Europe.

David had been a decorated fighter pilot and Air Force officer. In fact, during the 9/11 attacks, he was the general who scrambled fighter jets over Washington and ordered pilots to use their discretion to shoot down any passenger plane that threatened the city. But even as a commanding general, he refused to be chauffeured around. He loved taking the Metro.

At 4:58 p.m., a screech interrupted the rhythmic click-clack of the wheels as the driver slammed on the emergency brake. Then

came a cacophony of broken glass, bending metal, and screams as Train 112 slammed into something: a train inexplicably stopped on the tracks. The impact drove a thirteen-foot-thick wall of debris—a mass of crushed seats, ceiling panels, and metal posts—into Train 112 and killed David, Ann, and seven others.

Such a collision should have been impossible. The entire Washington Metro system, made up of over one hundred miles of track, was wired to detect and control trains. When trains got too close to each other, they would automatically slow down. But that day, as Train 112 rounded a curve, another train sat stopped on the tracks ahead—present in the real world, but somehow invisible to the track sensors. Train 112 automatically accelerated; after all, the sensors showed that the track was clear. By the time the driver saw the stopped train and hit the emergency brake, the collision was inevitable.

As rescue workers pulled injured riders from the wreckage, Metro engineers got to work. They needed to make sure that other passengers weren't at risk. And to do that, they had to solve a mystery: *How does a train twice the length of a football field just disappear?*

II.

Alarming failures like the crash of Train 112 happen all the time. Take a look at this list of headlines, all from a single week:

CATASTROPHIC MINING DISASTER IN BRAZIL

ANOTHER DAY, ANOTHER HACK: CREDIT CARD STEALING MALWARE HITS HOTEL CHAIN

HYUNDAI CARS ARE RECALLED OVER FAULTY BRAKE SWITCH

STORY OF FLINT WATER CRISIS, "FAILURE OF GOVERNMENT," UNFOLDS IN WASHINGTON

"MASSIVE INTELLIGENCE FAILURE" LED TO THE PARIS TERROR ATTACKS

VANCOUVER SETTLES LAWSUIT WITH MAN WRONGFULLY IMPRISONED FOR NEARLY THREE DECADES

EBOLA RESPONSE: SCIENTISTS BLAST "DANGEROUSLY FRAGILE GLOBAL SYSTEM"

INQUEST INTO MURDER OF SEVEN-YEAR-OLD HAS BECOME SAGA OF THE SYSTEM'S FAILURE TO PROTECT HER

FIRES TO CLEAR LAND SPARK VAST WILDFIRES AND CAUSE ECOLOGICAL DISASTER IN INDONESIA

FDA INVESTIGATES E. COLI OUTBREAK AT CHIPOTLE RESTAURANTS IN WASHINGTON AND OREGON

It might sound like an exceptionally bad week, but there was nothing special about it. Hardly a week goes by without a handful of meltdowns. One week it's an industrial accident, another it's a bankruptcy, and another it's an awful medical error. Even small issues

can wreak great havoc. In recent years, for example, several airlines have grounded their entire fleets of planes because of glitches in their technology systems, stranding passengers for days. These problems may make us angry, but they don't surprise us anymore. To be alive in the twenty-first century is to rely on countless complex systems that profoundly affect our lives—from the electrical grid and water treatment plants to transportation systems and communication networks to healthcare and the law. But sometimes our systems fail us.

These failures—and even large-scale meltdowns like BP's oil spill in the Gulf of Mexico, the Fukushima nuclear disaster, and the global financial crisis—seem to stem from very different problems. But their underlying causes turn out to be surprisingly similar. These events have a shared DNA, one that researchers are just beginning to understand. That shared DNA means that failures in one industry can provide lessons for people in other fields: dentists can learn from pilots, and marketing teams from SWAT teams. Understanding the deep causes of failure in high-stakes, exotic domains like deepwater drilling and high-altitude mountaineering can teach us lessons about failure in our more ordinary systems, too. It turns out that everyday meltdowns—failed projects, bad hiring decisions, and even disastrous dinner parties—have a lot in common with oil spills and mountaineering accidents. Fortunately, over the past few decades, researchers around the world have found solutions that can transform how we make decisions, build our teams, design our systems, and prevent the kinds of meltdowns that have become all too common.

This book has two parts. The first explores why our systems fail. It reveals that the same reasons lie behind what appear to be very different events: a social media disaster at Starbucks, the Three Mile Island nuclear accident, a meltdown on Wall Street, and a strange scandal in small-town post offices in the United Kingdom. Part One

also explores the paradox of progress: as our systems have become more capable, they have also become more complex and less forgiving, creating an environment where small mistakes can turn into massive failures. Systems that were once innocuous can now accidentally kill people, bankrupt companies, and jail the innocent. And Part One shows that the changes that made our systems vulnerable to accidental failures also provide fertile ground for intentional wrongdoing, like hacking and fraud.

The second part—the bulk of the book—looks at solutions that we can all use. It shows how people can learn from small errors to find out where bigger threats are brewing, how a receptionist saved a life by speaking up to her boss, and how a training program that pilots initially dismissed as "charm school" became one of the reasons flying is safer than ever. It examines why diversity helps us avoid big mistakes and what Everest climbers and Boeing engineers can teach us about the power of simplicity. We'll learn how film crews and ER teams manage surprises—and how their approach could have saved the mismanaged Facebook IPO and Target's failed Canadian expansion. And we'll revisit the puzzle of the disappearing Metro train and see how close engineers were to averting that tragedy.

We came together to write this book from two different paths. Chris started his career as a derivatives trader. During the 2007–2008 financial crisis, he watched from his trading desk as Lehman Brothers collapsed and stock markets around the world unraveled. Around the same time, he began to train as a pilot and developed a very personal interest in avoiding catastrophic mistakes. András comes from the world of research and studies why organizations struggle with complexity. A few years ago, he created a course called Catastrophic Failure in Organizations, in which managers from all sorts of backgrounds study headline-grabbing failures and share their own experiences with everyday meltdowns.

Our source material for the book comes from accident reports, academic studies, and interviews with a broad swath of people, from CEOs to first-time homebuyers. The ideas that emerged explain all sorts of failures and provide practical insights that anyone can use. In the age of meltdowns, these insights will be essential to making good decisions at work and in our personal lives, running successful organizations, and tackling some of our greatest global challenges.

III.

One of the first people we interviewed for this book was Ben Berman, a NASA researcher, airline captain, and former accident investigator who also has an economics degree from Harvard. In many ways, Berman explained, aviation is an ideal laboratory in which to understand how small changes can prevent big meltdowns.

Though the likelihood of a failure on an individual flight is vanishingly small, there are more than one hundred thousand commercial flights per day. And there are lots of noncatastrophic failures, occasions when error traps—things like checklists and warning systems—catch mistakes before they spiral out of control.

But still, accidents happen. When they do, there are rich sources of data about what went wrong. Cockpit voice recorders and black boxes provide records of the crew's actions and information about what was going on with the airplane itself, often all the way to the point of impact. These records are critical to investigators like Berman—people who dig through the human tragedy of crash sites to prevent future accidents.

On a beautiful May afternoon in 1996, Berman was in New York City with his family when his pager went off. Ben was on the National Transportation Safety Board's "Go Team," a group of

investigators dispatched in case of a major accident. He soon learned the grim details: ValuJet Flight 592, carrying more than one hundred passengers, had disappeared from radar ten minutes after takeoff from Miami and crashed into the Florida Everglades swamp. A fire had broken out on board—that much was clear from the pilots' radio calls to air traffic control—but what had caused it was a mystery.

When Berman arrived at the accident site the next day, the smell of jet fuel still lingered in the air. Debris was scattered over the dense marshes, but there was no sign of the fuselage or anything else that looked like an airplane. The fragmented wreckage was buried under waist-high water and layers of saw grass and swamp muck. Sneakers and sandals floated on the surface.

While search crews combed the black swamp water, Berman assembled his team at the Miami Airport and began to interview people who had handled the flight on the ground. One by one, ramp agents came to the ValuJet station manager's office, where the investigators had set up for the day. Most interviews went something like this:

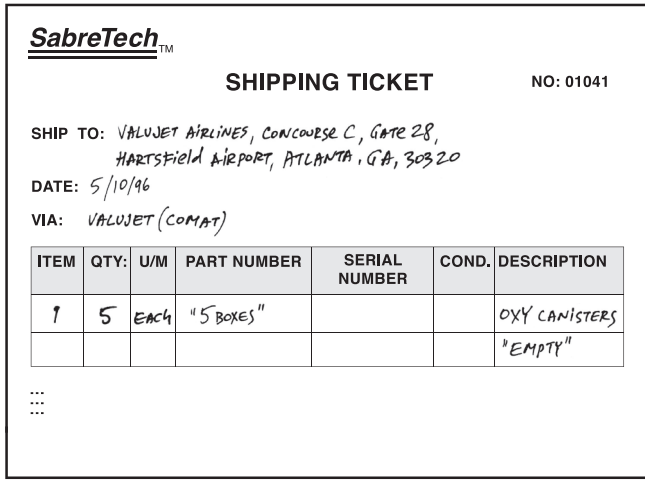
BERMAN: What did you notice about the plane?
RAMP AGENT: Nothing special, really . . .
BERMAN: Anything unusual when you were servicing the plane? Or when you were helping with the pushback? Or any other time?
RAMP AGENT: No, everything was normal.
BERMAN: Did *anything* at all draw your attention?
RAMP AGENT: No, really, there was nothing at all.

No one had seen anything.

Then, while sipping coffee between interviews, Berman noticed something interesting in a stack of papers on the station manager's desk. The bottom of a sheet stuck out from the pile, with a signature

on it. It was Candalyn Kubeck's; she was the flight's captain. Berman pulled the stack from the tray and leafed through the sheets. They were nothing special, just the standard flight papers for ValuJet 592.

But one sheet caught his attention:



SabreTech™

SHIPPING TICKET NO: 01041

SHIP TO: VALUJET AIRLINES, CONCOURSE C, GATE 28, HARTSFIELD AIRPORT, ATLANTA, GA, 30320

DATE: 5/10/96

VIA: VALUJET (COMAT)

ITEM	QTY:	U/M	PART NUMBER	SERIAL NUMBER	COND.	DESCRIPTION
1	5	EACH	"5 BOXES"			OXY CANISTERS
						"EMPTY"

It was a shipping ticket from SabreTech, an airline maintenance contractor, listing ValuJet "COMAT"—company-owned materials—that were on the plane. Berman was intrigued. There had been a fire on the plane, and here was a document saying there had been oxy canisters on board. And there was something else: "It was the quotation marks around 'empty' that got me," Berman told us.

The investigators drove over to SabreTech's office at the airport and found the clerk who had signed the shipping ticket. They learned that the items described on the ticket as oxy canisters were actually chemical oxygen generators, the devices that produce oxygen for the masks that drop from overhead compartments if a plane loses cabin pressure.

"So, were these empty?" Berman asked.

"They were out of service—they were unserviceable, expired."

This was a big red flag. Chemical oxygen generators create tremendous heat when activated. And, under the wrong conditions, the otherwise lifesaving oxygen can stoke an inferno. If the boxes contained expired oxygen generators—ones that reached the end of their approved lives—rather than truly empty canisters, a powerful time bomb might have been loaded onto the plane. How could this happen? How did this deadly cargo find its way onto a passenger jet?

The investigation revealed a morass of mistakes, coincidences, and everyday confusions. ValuJet had bought three airplanes and hired SabreTech to refurbish them in a hangar at Miami Airport. Many of the oxygen generators on these planes had expired and needed to be replaced. ValuJet told SabreTech that if a generator had not been *expended* (that is, if it was still capable of generating oxygen), it was necessary to install a safety cap on it.

But there was confusion over the distinction between canisters that were *expired* and canisters that were not *expended*. Many canisters were expired but not expended. Others were expired and expended. Still others were expended but unexpired. And there were also replacement canisters, which were unexpended and unexpired. "If this seems confusing, do not waste your time trying to figure it out—the SabreTech mechanics did not, nor should they have been expected to," wrote the journalist and pilot William Langewiesche in the *Atlantic*:

> Yes, a mechanic might have found his way past the ValuJet work card and into the huge MD-80 maintenance manual, to chapter 35-22-01, within which line "h" would have instructed him to "store or dispose of oxygen generator." By diligently pursuing his options, the mechanic could have found his way to a different part of the manual and learned that "all serviceable and unserviceable (unexpended) oxygen generators (canisters) are to be stored in an area that ensures that each unit is

> not exposed to high temperatures or possible damage." By pondering the implications of the parentheses he might have deduced that the "unexpended" canisters were also "unserviceable" canisters and that because he had no shipping cap, he should perhaps take such canisters to a safe area and "initiate" them, according to the procedures described in section 2.D.

And this just went on: more details, more distinctions, more terms, more warnings, more engineer-speak.

The safety caps weren't installed, and the generators ended up in cardboard boxes. After a few weeks, they were taken over to SabreTech's shipping and receiving department. They sat there until a shipping clerk was told to clean up the place. It made sense to him to ship the boxes to ValuJet's headquarters in Atlanta.

The canisters had green tags on them. Technically, a green tag meant "repairable," but it's unclear what the mechanics meant by it. The clerk thought the tag meant "unserviceable" or "out of service." He concluded that the canisters were empty. Another clerk filled out a shipping ticket and put quotation marks around "empty" and "5 boxes." It was just his habit to put words between quotation marks.

The boxes traveled through the system, step by step, from the mechanics to the clerks, from the ramp agents to the cargo hold. The flight crew didn't spot the problem, and Captain Kubeck signed the flight papers. "As a result, the passengers' last line of defense folded," wrote Langewiesche. "They were unlucky, and the system killed them."

THE INVESTIGATIONS into Washington Metro Train 112 and ValuJet 592 revealed that these accidents were rooted in the same cause: the increasing complexity of our systems. When Train 112 crashed, Jasmine Garsd, a producer at National Public Radio, happened to be

riding a few cars back from the impact. "The train collision was like a very fast movie coming to a screeching halt," she recalled. "I think in moments like these you come to realize two things: how tiny and vulnerable we are in this world of massive machines we've built, and how ignorant we are of that vulnerability."

But there is hope. In the past few decades, our understanding of complexity, organizational behavior, and cognitive psychology has given us a window into how small mistakes blossom into massive failures. Not only do we understand how these sorts of accidents happen, but we also understand how small steps can prevent them. A handful of companies, researchers, and teams around the world are leading a revolution to find solutions that prevent meltdowns—and don't require advanced technologies or million-dollar budgets.

In the spring of 2016, we arranged for Ben Berman to speak to a room full of people interested in the risk management lessons of aviation. It was an incredibly diverse group: HR professionals and civil servants, entrepreneurs and doctors, nonprofit managers and lawyers, and even someone from the fashion industry. But Berman's lessons cut across disciplines. "System failures," he told the group, "are incredibly costly and easy to underestimate—and it's very likely that you'll face something like this in your career or your life." He paused and looked out at the audience. "The good news, I think, is that you can make a real difference."