ArchBridge Family Office

Accidents Will Happen: Why Things Keep Breaking, and Why We Should Expect More

I was nine years old in 1979, and that was the year I became terrified of nuclear reactors.

We were in the middle of the Cold War, and I was already scared of a nuclear war with the Soviet Union. Then, over about two weeks that spring, nuclear power plants moved near the top of my boogeyman list.

First came *The China Syndrome*. It opened on March 16, 1979, starring Jane Fonda, Michael Douglas, and Jack Lemmon, and it was about a near-meltdown at a nuclear power plant. The title came from the idea that an uncontrolled nuclear core could burn through the Earth all the way to China. (Of course a reactor core couldn't plow all the way through the planet. And if it could, you'd come out in the Indian Ocean southwest of Australia. China isn't even on the other side.)

Twelve days later, life imitated art. On March 28, a stuck valve at the Three Mile Island plant near Harrisburg, Pennsylvania, allowed cooling water to escape from one of the reactors. Operators misread the situation, and by the time they restored coolant flow, about half the core had melted. Nobody died, but it was the worst nuclear accident in American history, and it felt like the movie had come true.

The country turned against nuclear power. Public support fell from 69% in 1977 to 46% in 1979. Orders for new reactors, which peaked at 41 in 1973, dropped to zero in 1979, and more than 100 planned reactors were eventually canceled. Today, nuclear power supplies about 18% of America's electricity. In France, it supplies about two-thirds.

Normal Accidents

Charles Perrow, a Yale sociologist, was asked to write a background paper for the presidential commission investigating Three Mile Island. That work became a 1984 book titled *Normal Accidents*, which I wrote about on my blog in 2019.

Perrow argued that some accidents aren't caused by a single bad operator or a single broken part. Instead, accidents are built into the system. Specifically, if a system has two features, something will eventually go wrong in a way nobody predicted.

The first feature is complexity: lots of parts interacting in ways that are hard to see. The second is tight coupling: the interrelated parts depend on each other so closely that there's no time or slack to fix a problem before it spreads. For example, a rocket launch is tightly coupled because every step must happen in order and at exactly the right moment. In contrast, a university is complex but loosely coupled. If a class you need is full, you can take it next semester.

Three Mile Island was both highly complex and tightly coupled. A maintenance mistake, backup pumps whose valves had been left closed after servicing, and a warning light hidden behind a repair tag combined in a way nobody had anticipated.

Counterintuitively, adding safety measures can make things worse because every new safety system adds complexity. As the risk manager Richard Bookstaber put it, "for every step in improving safety or monitoring potential failures, they introduce their own sources of failure." Keep that in mind. It matters for what happened last week.

Perrow put nuclear plants in the most dangerous category, both complex and tightly coupled, and he argued that some technologies should simply be abandoned. The U.S. more or less took that advice on nuclear reactors. France didn't.

The Financial Crisis Was a Normal Accident, Too

Perrow wrote about power plants, dams, and airplanes. Bookstaber applied the same idea to financial markets in his 2007 book, *A Demon of Our Own Design*. It came out about a year before the financial crisis, and it read like a forecast.

The complexity was in the products. Mortgages were bundled into securities; those securities were sliced up and bundled again, and credit default swaps insured the risk. By the end, almost nobody could tell who would lose money if a homeowner in Las Vegas defaulted.

The tight coupling came from leverage and short-term borrowing. Some Wall Street firms borrowed $30 or more for every dollar of their own, and much of that debt had to be rolled over every night. When the losses showed up, lenders pulled back, and firms had to sell whatever they could. Lehman Brothers filed for bankruptcy on September 15, 2008. The next day, the government rescued AIG, which had insured a big share of everyone else's bets. It was like dominoes falling.

And just as Perrow would have predicted, the things meant to make the system safer, like AAA ratings and insurance against default, added complexity and spread the damage.

Nassim Taleb gave us useful words for this in his book *Antifragile*. Some things are fragile, like a wine glass: a shock breaks them. Some are robust, like a rock: a shock doesn't do much. And some are antifragile, like muscles: stress makes them stronger. The big banks in 2008 were fragile. They had been built for efficiency, with no slack.

What's Happening Now

Which brings me to last week.

On Monday, a problem at Chase spread into delays at other big banks. On Tuesday, Apple blamed an internal update for problems with the App Store and iCloud sign-ins, and an NSA system for classified messages went down. On Thursday, Microsoft's email went down around the world. On Friday, the FAA stopped departures nationwide, and more than 18,000 U.S. flights were canceled between Friday and Sunday. (I was one of the people stuck on a tarmac at O'Hare.)

These incidents sure looked connected. But the people in a position to know said it wasn't. Secretary of State Marco Rubio said the government had "zero evidence" the events were connected. Chris Krebs, who used to run the federal government's cybersecurity agency, put it more bluntly: "Everybody just needs to chill out for a second."

Despite the reassurances from the government and various experts, could the disruptions over the past few weeks be targeted cyberattacks? Yes. That is possible. But the more likely scenario is that we're seeing exactly what Perrow would have predicted. Anjana Rajan, a former Biden administration official and CEO of the cybersecurity company Atalanta, said, "We're asking too many questions about who did this, rather than, do I even understand what my systems are doing under normal, abnormal or hostile conditions. When you start to have these really complex, sprawling, software-defined systems that are all interconnected, it's very hard to understand them."

Exhibit A is air traffic control. In 2024, the Government Accountability Office found that 105 of the FAA's 138 air traffic control systems were unsustainable or potentially unsustainable. Some still ran on floppy disks and paper strips. The FAA has been racing to modernize, including swapping 5,170 copper lines from the 1960s for fiber optic cable. In September, the GAO warned that the rush could disrupt air traffic. Then the ground stop happened while a contractor was moving lines from copper to fiber at a remote site. The upgrade caused the break.

The other outages followed the same pattern. Microsoft said it had brought new servers online before its outage. Chase blamed a software bug. Apple blamed an internal update. These likely weren't attacks. They were companies changing complicated systems that a lot of other things depend on.

Now add AI. AI tools have gotten very good at finding security holes in old software. The cybersecurity world nicknamed last month "Black October" because so many serious vulnerabilities were found and fixed, many of them by AI. Microsoft's October update alone fixed more than 1,400. Every one of those fixes is a safety measure. And each one changes old, interconnected systems. Senator Mark Warner said the pressure was "putting tremendous strain on systems that weren't built to handle that pace of change."

That's Bookstaber's point. The fixes bring their own sources of failure.

So put it together. We have old systems that were never designed for this, new technology layered on top of them, and AI forcing changes faster than ever. And it's all tightly connected, so a problem at one company spreads to others. That's a recipe for normal accidents, and I expect we'll see more of them.

The Bad Guys Haven't Gone Away

None of this means we can stop worrying about hackers or rogue AI. We're also in an on-and-off war with Iran, and the U.S. resumed strikes right after the midterms. Iranian-linked hackers have already disrupted U.S. water and energy systems this year and will almost certainly keep trying to cyberattack the US. Just before the latest outages, the FBI warned about an AI platform that criminals had used to automate cyberattacks at "machine speed." Someone will eventually try to take down a bank, a utility, or part of the power grid. Both things can be true: systems will break on their own, and people will try to break them.

The good news is that the preparation is mostly the same either way. In my last article, Taking My Own Advice, Nine Years Late, I wrote about what my family has done at home: some cash, a solar power bank, water, food, and N95 masks. That covers the household. Here's what I'd do with the portfolio.

Add slack. Perrow had two pieces of advice for living with normal accidents: make the system simpler, or add slack. We can't simplify the world's technology. But we can add slack to our own finances.

Diversify. Don't depend on any one company, asset class, or institution. Own bonds in addition to stocks. When something breaks, you want it to be one piece of your financial life, not the whole thing.

Keep at least a year of portfolio withdrawals in cash. If you're living off your portfolio, setting aside a year or more of spending means a market panic, or a week when your bank's website won't load, doesn't force you to sell at the worst possible time. A forced seller is tightly coupled to the market. Someone with a year of cash isn't. And if markets do go haywire, that cash lets you buy when others have to sell. That's about as close to antifragile as most of us will get.

Go easy on leverage. Bookstaber called leverage one of the key ingredients of tight coupling. It's what turned 2008 from a bad year into a crisis.

When I was nine, my answer to Three Mile Island was fear. Forty-seven years later, my answer is more practical: a diversified portfolio, a year of withdrawals in cash, and a basement with water jugs and a solar-powered battery backup. Accidents will happen. I'd rather have some slack when they do.

ArchBridge Family Office is an independent, multi-family office and trust company that advises 65 clients on more than $13 billion of investment assets and more than $16 billion of total wealth. Founded in 2002, ArchBridge Family Office provides holistic, high-touch client service including customized, independent investment management and a full range of family office and fiduciary services. The firm serves a limited number of clients with substantial wealth in order to maintain very low client-to-employee ratios. Visit archbridge.com to explore how the firm manages complexity with unmatched expertise and a Family, Forward focus.