Taking My Own Advice, Nine Years Late: Preparing for Cyberattacks, Pandemics, and Power Outages Without Building a Bunker

In May 2017, I wrote a blog post titled "Pandemic Preparedness 101." I advised readers to stock at least two weeks of food and a gallon of water per person per day. Keep a battery-powered radio, a first-aid kit, and extra medications. Have cash on hand in case ATMs go down. Consider buying face masks. I noted that following this advice was "cheap and easy to do!!!!" Yes, I had four exclamation marks.

Then I did none of it.

Three years later, COVID-19 arrived, and I found myself wishing I'd listened to my own advice.

A Dress Rehearsal

Last Thursday, I was in Wichita, giving a speech about my upcoming book on wealth and happiness. That same day, Microsoft Outlook went down. What started as an email problem in the Americas spread into a worldwide outage across Microsoft 365 and dragged into Friday because the fixes didn't hold.

On Friday, I flew home through Chicago and got stuck because of the nationwide ground stop. My plane sat on the tarmac at O'Hare for three hours because the nation's air traffic control centers had failed. Airlines canceled more than 12,000 flights.

I should confess that my personal suffering was minimal. I was in first class with a book, noise-canceling headphones, and a few IPAs. When it became clear I wasn't flying anywhere, I booked a hotel room, and the next day I took Amtrak home to St. Louis. It was five hours, and I enjoyed it immensely.

It wasn't just Microsoft and the FAA. Two days before my speech, Apple's iCloud went down for about two hours, taking email, photos, and sign-ins with it. And on Monday, customers at Chase, Wells Fargo, Bank of America, and other large banks couldn't check balances or move money.

These incidents made me think. None appears to have been an attack. Microsoft reported no signs of malicious activity, the FAA's early investigation pointed to a new router being installed at a site in Arkansas, and Chase blamed a software bug. The common thread so far is companies upgrading or patching old systems. So these were just technology glitches with huge consequences. The Microsoft outage knocked out email for businesses worldwide, and the FAA's outage threw American air travel into chaos for a few days. I understand why people are uneasy.

Now Imagine Someone doing It On Purpose

A few days before my trip, The Atlantic ran a piece by Matteo Wong titled "Prepare for the AI Apocalypse Like You'd Prepare for a Snowstorm." He reported several AI-related incidents:

- AI was recently used to uncover major security flaws in software running on 70 percent of websites. The NSA told organizations to patch the flaw immediately or take their systems offline. The bug had been sitting in the code for 14 years.
- Attackers drained billions of dollars from the crypto exchange Binance, in part by hijacking the company's own AI tools.
- This summer, cyberattacks disrupted water utilities across the country.

Then there are the freezers. In October, hackers took control of the refrigeration systems in hundreds of French supermarkets. Two weeks ago, it happened again in at least seven more European countries, including Belgium, Sweden, and Ireland. Freezer temperatures were pushed as high as 122 degrees, and stores threw out spoiled food. The FBI has since warned that industrial refrigeration systems worldwide may be targets.

All those incidents involved human bad actors. The story that sticks with me most didn't even involve a human. In July, an AI model OpenAI was testing escaped its test environment and broke into Hugging Face, a platform that hosts AI models. Over four and a half days, it took some 17,600 actions inside systems it was never supposed to reach. Nobody told it to attack anyone. It was taking a cybersecurity exam and broke in to steal the answer key.

Now imagine bad actors, human or AI, taking aim at the financial system, the power grid, fuel, or transportation. Picture the disruption lasting two weeks instead of the two days the Microsoft and FAA snafus persisted.

Another pandemic could happen, too. COVID-19 may well have originated in a lab in China. Last month, a researcher at an anti-plague laboratory in Siberia died of an unexplained infection following a reported lab accident. The Russian incident reminds us that it could happen again. Or the next one could arise naturally.

A Snowstorm or a Hurricane, Not a Bunker

I wrote a whole book about uncertainty and the difficulty of predicting the future, so I have no idea whether the next disruption will be a hack, a virus, a hurricane, or another technology snafu. The good news is that we don't need to know. That's why Wong advises preparing the way you would for a snowstorm. A disaster-preparedness expert quoted in the Atlantic piece makes the point well: if your power is out, it hardly matters whether an earthquake or a cyberattack caused it. The same modest supplies cover all of them.

The article also describes how far some people in Silicon Valley go, with remote bunker plans and stockpiles of guns, gold, and gas masks. That's not what I'm suggesting here. If going further helps you sleep, that's your call, and I'm not judging. People draw this line in different places. My point is that you can be in good shape without going anywhere near that far.

What I Did This Time

Unlike in 2017, I've actually acted on my own advice. Over the past couple of weeks, I've done six things:

1. **Cash.** I keep extra cash at home in fives, tens, and twenties. If card networks or ATMs go down, cash still works. How much? A common guideline is to keep enough to cover two weeks of everyday spending, such as groceries, gas, and prescriptions. Depending on your household, that's somewhere from $1,000 to $10,000. I wouldn't keep much more than that at home, and you should store it in a fireproof safe.
2. **Power.** I bought a Jackery HomePower 1000 Plus v2 with an add-on battery pack and two folding 200-watt solar panels. It's a large portable rechargeable battery that sits in the basement until I need it, and the panels recharge it from the sun. It will run the refrigerator, internet, lights, and phones for a couple of days, and longer when the sun is out. It needs no gas and no installation.
3. **Masks.** I stocked up on N95s. In 2020, you couldn't find them. Today a box of ten costs about $25.
4. **Food.** I bought freeze-dried meals and extra canned food. The canned food is stuff we already eat, so we'll rotate through it.
5. **Water.** I bought six Saratoga Farms 5-gallon stackable water containers, which hold 30 gallons. Add the water sitting in our water heater and we have a few weeks of drinking water. WaterBricks are another good choice. They're smaller, at 3.5 gallons each, and they stack like Legos. I also bought a water filter that makes it safe to drink from a stream, lake, pond, or suspect tap water.
6. **Prescriptions.** We're stockpiling prescription meds by paying out of pocket for extra months. We've found that Amazon Pharmacy works well for this. You can also ask your doctor for 90-day refills, which many insurers cover.

The specific products noted above aren't recommendations from ArchBridge. They're simply what made sense for my family, and the products I mention are just the ones I happened to buy. Neither the firm nor I have any relationship with these companies.

All of it fits on a few basement shelves. None of it was hard, which is roughly what the 2017 post said, minus the exclamation points.

The Digital Side

The Atlantic piece says the easiest and possibly most important step is getting your digital house in order. Use a different password for every account and store them in a password manager such as Dashlane, 1Password, or LastPass. Turn on two-factor authentication, preferably via an app. Keep your phone and computer updated. Save offline copies of the photos and documents you'd hate to lose (buying an external hard drive for this is a good idea).

Be wary of anyone who contacts you. AI can now clone a voice from a short recording, so a familiar voice asking for money proves nothing. If your bank calls, hang up and call back using the number printed on your card. Agree on a family code word that a caller must know before anyone sends a dime.

An Hour at the Computer

Getting ready is easier than you'd think. Almost everything on my list can be ordered on Amazon or elsewhere online, so you can sit down for an hour and knock out most of it at once: water containers, masks, food, and a password manager. The cash requires one trip to the bank (or many trips to the ATM if your bank, like mine, doesn't have branches).

The expert in the Atlantic article says the most important preparation is knowing your neighbors because connected communities fare better through disasters. I like that the top item on the list costs nothing.

In 2017, I wrote the list. This time, I'm working through it. With any luck, the masks will gather dust and the freeze-dried lentil stew will expire unused.

The views in this article are the author's own and are shared for general information only. They are not individualized advice. ArchBridge Family Office does not endorse any product, service, or company mentioned and receives no compensation from any of them. Your own needs may differ.

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.