/dev/random
Cloudbursting, or Risk Mismanagement

ROBERT G. FERRELL

Robert G. Ferrell is a fourth-generation Texan, literary techno-geek, and finalist for the 2011 Robert Benchley Society Humor Writing Award. rgferrell@gmail.com

As I write this, my area is still recovering from Hurricane Harvey, while Floridians are sloshing their way out from under Irma. People who choose to live in places like this are perfectly well aware that sooner or later we're going to get smacked by a tropical weather system, however. It's a risk we all accept and manage—with varying degrees of skill.

I built my former career on risk and the mitigation thereof. Well, at least the second half of it or so. Before that I was an analytical chemist, colon cancer researcher (which largely entailed cleaning up radioactive rat poop), percussionist, professional grad school dropout (three different programs), and probably some other stuff I don't remember. But (as I expect it will say on my epitaph), I digress. (Sorry for all the asides: I had some parentheses in stock that had reached their "use-by" date. Waste not, want not.)

We all take risks. Heck, just by reading my column you're risking long-term neocortical damage. If you don't work from home (or, if your house is as cluttered as mine, even then), you're taking a substantial risk just traveling to your place of employment. Yes, really. Have you seen the way some of those people out there drive? The other day I spotted a doofus sitting in the driver's seat of a big truck while yakking on the cell phone and apparently watching a DVD on the little screen perched on his dashboard. (I hesitate to say he was "driving" the truck, because I don't think that's an accurate assessment.) Maybe it was a defensive driving video, I don't know. Regardless, it did not appear that keeping his vehicle between the lines, or even on the asphalt, was high on his priority list. I just pulled over to a rest area for a few minutes to give him time to have his accident without me. Not that you could really call it an "accident": more like a "grossly negligent."

Horrifyingly bad drivers illustrate the category of existential risk we can't realistically avoid. Another member of this set is what I refer to as a "cloudburst," or loss of personal data entrusted to some third party without the owner's explicit awareness. No matter how diligently you ensure that your connection to a first-line merchant or financial provider is protected by SSL/TLS/whatever with valid certificates, you have zero control or even in most cases cognizance of what happens to that precious information once you've transferred it thusly. It is now completely at the mercy of any thief who manages to defeat the safeguards of nebulous third parties. It's somewhat like carrying your cash to the bank in an armored car only to have them store it in the lobby, "protected" by cardboard boxes marked Please Do Not Steal.

If you decide to go that extra diligence mile and track your data beyond the first step, good luck. Most institutions are extremely reticent when it comes to sharing details of their processing chain, for "security" reasons. That is, they don't want you to know that there really isn't much of that going on. "That's not something you should worry your pretty little head about," they'll say condescendingly, "We've got it under control," and give you a big thumbs up. The next week you receive an email informing you that your account was one of 200 million compromised—and here's a year of free credit monitoring, not that it will do you much

good. I think I've had free credit monitoring for almost a decade now because of these little serial overlapping "security incidents," and all I've gotten out of it were a long string of warnings and vague reassurances.

The "cancel every credit instrument and change all 85 of your online passwords" circus is getting to be far too routine for my taste. Some of my credit cards are on their fourth or fifth iteration, all because various financial processing entities along the path of ignominy couldn't keep their security diapers pinned.

What is the fundamental malfunction with these firms/agencies? Why are they taking so many liberties with our precious data? I don't know: hubris, maybe, or perhaps our old scabrous nemeses ignorance and indolence. Whatever the case, compromise is the new norm. A foreign government lacking even the pretense of having my best interests at heart, for example, now possesses the volumes of incredibly intrusive information I supplied to get the security clearance I held in my former career. The irony of a government that can't keep its own barn door shut questioning me at length about my ability to preserve secrets would be laughable if it weren't so egregious. At least when I got read onto a SAP (Special Access Program), I didn't turn around and store the relevant info on Dropbox with the password "Unc73$4M," 'leet-speak for Uncle Sam.

So, what can we, as information technology professionals, do about this—apart from posing largely rhetorical questions? While constantly increasing both encryption key lengths and the complexity of passwords may give senior management, stockholders, and legislators a warm fuzzy, the real answer lies in educating the people along that data processing path. Technology, regardless of how well designed or robustly implemented, cannot take the place of human security awareness. These protocols and hardware devices and algorithms are only as effective as the people who deploy them. It is evident that if we don't change the way rank and file employees think about and implement data security, any reasonable expectation of identity fidelity is but a fool's dream. No matter how sharp your plow or powerful your oxen, the furrows you dig will not yield any crops if the soil itself is poor. (Mmm. Pre-industrial agriculture analogies always make me hungry. Fortunately, I keep a pot of gruel going next to my computer for such contingencies.)

The state of Illinois is reportedly working on employing blockchains to provide a "sovereign digital identity." I applaud this effort and any others that help us move away from static identifiers like Social Security numbers that, once compromised, become liabilities rather than authenticators. They are, in effect, lifelong passwords you can't (easily) change.

If you are one of those third-party data-manglers, my suggestion for storage of personally identifying information is to use a randomized multicontainer approach. With SSNs, for example, you could split the numbers into chunks of two digits and then randomly store each chunk in one of five containers. You could use the same algorithm with name or other data fields, actually, except that the string length would be variable. Unique identifiers would therefore be serial numbers containing the location and position within the string (and in some cases, length) of each chunk. You'd have to map the positional data for name and SSN in a relational database of some kind, of course, but your network folks already more or less do that with NAT, so that will be familiar ground. You could even craft said UIDs in the same format as SSNs, to confuse thieves into thinking they've stolen the data, rather than the pointer.

Or you could just stop opening attachments and using Pirate Bay torrents at work. I don't want to suggest anything too outlandish and ridiculous, however. Even humorists have their limits.