WeGet letters

by Michael W Lucas

Dear Opinionated Doofus,

You've said a bunch of stuff against encrypting your disks. Are you crazy? With the world we live in, we absolutely need storage encryption.

—Encryption4Life

Dear Whatever,

The answer to the question you asked is obviously "yes."

Don't know what the other statements had to do with anything.

Dear Opinionated Doofus,

You wanna be that way? Fine. Do you honestly believe that encrypting disks is not worthwhile?.

—Encryption4Life

Dear Congratulations-on-Learning-to-Ask-a-Question,

This is two questions. The answer to the first is, again, yes.

As for the second:

The hard part of writing this column has nothing to do with putting the words together, explaining the technology, or dealing with our cutting-edge technology that's barely a sneeze from toppling over. No, it's pretending that I care what people think. Upon seeing my cheerful expression of incipient bucolicism, readers erroneously conclude that I'm amenable to their inadequately brewed opinions. In truth, I've learned that maintaining a gormless façade is all that protects and preserves my tolerable existence wedged in the Writing Pit against the League of Extraordinary Grumps declaring me their Grand Fiend by snarling acclaim.

If you think you need disk encryption everywhere, go for it. I won't argue with you. I can't be troubled.

Most at-rest disk encryption isn't useful for most people, though. And most environments where it would be useful don't use it.

Encryption is a response to a threat. Some of those threats are real. Some are not. Some of those threats are targeted at us. And everyone must balance different threats.

Some people have real, physical threats. Relief workers in war zones need encrypted storage. It won't save them, but might well save their coworkers, peers, and those they succor. Their computers are often offline or connect to the Internet only on occasions when the satellite uplink happens to be working and the ongoing atrocities have slowed to a trickle.

Folks with more connected lives face different threats. Disk encryption prevents some of them.

Disk encryption is great against random theft. If you carry confidential or sensitive documents on your laptop, disk encryption will keep a lucky mugger from uploading them to

WikiLeaks. Most muggers who discover that your laptop doesn't run a "normal" operating system will not consider themselves lucky. They will wipe the disk, saving you the worry.

Disk encryption is great for data you want to deliberately destroy. If your organization is bound by rules declaring decommissioned disks must be overwritten with garbage when removed from service, encrypting the disks at installation is proactive scrambling. Once you destroy the keys, the disks are unreadable.

For most people, key destruction is the problem.

Or rather, key loss.

People have this horrid habit of living at the outer limit of tolerable complexity. We keep claiming ownership of problems (usually branded as "opportunities") until we pick up one too many and complain that we are swamped, overwhelmed, and incapable of handling anything else. At that point, much like pushing two-gigabit through a one-gigabit link, we start dropping packets. Encryption key management is one of these packets. If you are going to use disk encryption, you must dedicate time and mental energy to managing and sustaining those keys.

I have known four people who legitimately manage their disk encryption keys and who regularly and demonstratably dedicate time, effort, and mental attention to the task. Three of them managed their disks under contract with their employment. The last was a successful union organizer who had been threatened and stalked by company owners.

I know many people who claim to manage their keys properly. Of those who make such claims, a substantial portion lose their decryption keys and their data. I've never performed a statistical analysis because I can't be bothered. Many recovered trivially because their data was not worthwhile. Others recovered trivially because the important chunks of data were backed up elsewhere.

Others lost critical data and never recovered it, because they allowed their lives to become overly complex and failed to maintain that encryption.

With a bunch of work, you could attract the attention of a nefarious, three-letter agency, a criminal cabal, or an organization rejected by Robert Ludlum as too ridiculous for his worst novel. Anyone reading this column has left fingerprints all over the Internet. You send all your traffic over onion routing? They'll skip identifying you by IP address and use personal information. On the darknet, nobody knows you're a Fed.

So, if you're under serious threat?

Take the threat seriously. Devote time, energy, and attention to it.

If your disk is fully encrypted, are your backups? How are those backups stored? Where are they? And who is pursuing you? Your data is only as secure as the least protected mechanism.

I'm all for privacy. I'm all for experimenting with disk encryption, discovering how much attention it demands, and learning if it's worthwhile for you. Discovery of data on your hard drive can threaten your privacy. Next to advertising networks and Internet-connected refrigerators, though, your hard drive is a trivial risk. You don't need to remember your secrets; any number of globe-spanning megacorps will do it for you!

How are the keys stored? On a can-opener flash drive you snagged at a random vendor's table at a slightly less random trade show? Forget the possibility that the flash drive contains malware. Is the drive reliable? I'll answer that for you: no, it's not. You need at least one backup key. You must regularly verify that the backup still works. That backup media is probably also as dubious as an Oracle salesman under quota the night before quarter end, so you need to be able to create new backup keys on media that will hopefully remain less defective for at least a day or two.

How are those backups protected?

Maybe you don't have a key on removable media. Perhaps your key is a passphrase. Only you know the passphrase. If you are seriously threatened, what will you do when a bunch of goons break out their Human Decryption Toolkit (a rubber hose, a pair of pliers, and an assortment of pointy bits they got off the free coupons at Harbor Freight)?

Maybe your threat comes from the sort of people who need warrants. Those people have learned how to seize your laptop while it's running.

Should you surrender your privacy and your data? No.

Should you protect it with disk encryption? Only if that's a real threat to your well-being. How do you know if it's a real threat? If you're willing to dedicate a slice of your precious complexity tolerance to maintaining that encryption, and actually carry out that maintenance, it's a real threat. Otherwise, it's a learning experience.

In truth: anything on a networked computer is not truly private.

No wonder the League of Extraordinary Grumps wants me.

Have a question for Michael?
Send it to letters@freebsdjournal.org

MICHAEL W LUCAS (https://mwl.io)'s newest books are *Sudo Mastery, 2nd Edition* and *Terrapin Sky Tango*.