When the cloud goes dark

The risk hiding in your construction software.

By **Tony Wright**, AMELIE·AI. Over forty years in construction, from site engineer to project manager.

In the early hours of 10 March 2021 a fire broke out at an OVHcloud data centre in Strasbourg. By morning a five-storey building was gutted and around 3.6 million websites were offline. Some never came back. All data and backups in the destroyed building were lost, and worst of all, some firms had paid extra for a backup that had been kept in the same building as the live data, so the fire took both. A French court later ordered damages, and more than 130 customers joined a class action.

When we say a thing is "in the cloud", what we hear is that it is safe. The fire did not read anyone's assumptions. This note is not anti-cloud. The cloud earns its place for shared models, drawings on a phone, and a genuine offsite copy. The point is narrower: which of your assets can you not afford to lose access to, and is it wise to keep those where you do not control them?

1. The cloud can fail, and take your data with it

A copy that shares its fate with the thing it protects is not a backup, it is proximity with better branding. Hardware fails, buildings burn, a bad configuration wipes a volume. If your only copy and your backup live inside the same provider, one bad night can end both, with no warning and no vote.

2. Your data is a target, and a hostage

Centralise everything online and you build one rich target. In December 2019 Canada's Bird Construction was hit by Maze ransomware, about 60GB encrypted, roughly nine million Canadian dollars demanded. In January 2020 the same gang struck Bouygues Construction, around 200GB locked, systems shut down worldwide. That May, UK firms BAM Construct and Interserve were each hit and had to shut systems down. Modern ransomware copies your files before it locks them and threatens to publish them, so one breach can freeze the job and hand your commercial position to the other side.

3. You are renting, not owning

This is the "limited access to your own data" problem made literal. In February 2016 Autodesk stopped selling new perpetual licences and moved to subscription only, raising prices around five per cent a year since, with a single AutoCAD seat now on the order of two thousand pounds a year. Rent, and you own a monthly permission, not a thing with value. Let it lapse and access can stop, and files made in that software can become hard to open. The key belongs to someone else, and the rent only rises.

4. And when the signal drops

A cloud-only tool needs a connection. On a remote site, a basement, a tunnel, or an inner-city plot behind thick concrete, and during the vendor's own outages, you cannot open the very plan you are on site to run.

The honest other side

Holding your own data is not a free pass. Once the file lives on your machine, backing it up is your job, and a lost laptop with no copy is nobody's fault but yours. The choice is not "cloud bad, local good", it is about control. A copy on your own drive, and a second on a cheap disk or memory stick, is not hostage to a subscription, not exposed to a stranger's data-centre fire, and not sitting in a honeypot. You carry the responsibility, and you carry the keys.

Where AMELIE·AI fits

Planning, scheduling and site tools that run 100% offline on your own Windows machine. Your project never leaves the device, there is no account and no cloud to breach, and you buy once instead of renting permission to your own work.

Site records are sealed with a tamper-evident fingerprint you hold, not a vendor. Free trial on the Microsoft Store. Forensic instruments by arrangement.

Microsoft Store: AMELIE.AI apps · amelie-ai-apps.netlify.app

Sources, all verified. OVHcloud fire: Datacenterdynamics, Blocks and Files, Uptime Institute, Wikipedia. Construction ransomware: Engineering News-Record, Construction Dive, iTnews, Bluebeam. Autodesk: Autodesk SEC filings, Digital Engineering 24/7.

General information only, written from experience and the public sources above. Not legal, financial or IT security advice. Take professional advice for your own circumstances.