



In the Swiss Fort Knox bunkers, the stored data is not only safe from non-authorized access but also from possible military and civil threats. Radioactive and electromagnetic forces are screened off, as well as impacts from natural catastrophes.

How your data can survive natural catastrophes and Murphy's Law

Wouldn't it be reassuring to know that your data could survive an earthquake, a flood or an atomic catastrophe? The firm Swissvault preserves and protects your data against loss in all eventualities, even against an office fire or a computer crash, which often have disastrous consequences.

□ By Nicole Maron, translated by Diana Oehrli

Important corporate data must be backed up daily. Nobody knows this better than Christoph Oswald, director of the company Swissvault AG. But a backup alone is not enough. Oswald advises urgently to

store one copy of your data in a secure place at least once a week. "Often, multiple mishaps occur simultaneously," Oswald said, "as is according to Murphy's Law." For example: "A backup becomes unreadable when (and

only when) you need it. When you want to replay a backup, you realize that the only 'restore' version was on the hard drive (and only there) before you formatted it. Your backup program
continued on page 4

continued from page 1

overwrites the only secure backup copy without your command. The most important data exists on the last, undetectable tape." In order to help clients from experiencing such negative experiences, Swissvault developed the Backup Butler, which relieves companies of any size as well as private persons of the daily backup task, all the while ensuring that the data in question is stored in the safest data center in all of Europe.

Highest security level avoids virtual and physical invasion

The data center run by Swissvault is the most secure of its kind in Europe and is known as Swiss Fort Knox. It is to be found in two secret locations in the Bernese Oberland. Deep in the mountains lies the data that would not only survive the end of the world, but also an attack from unauthorized persons. An usually high 448-bit encryption protects from hackers, and a five-level security control protects the data bunker from physical entry: to go through the first armored door, one must be accompanied by security personnel and a security manager; the second armored door will only open once the first door is closed. A third armored door weighing 3.5 tons can only be operated by a guard, because the hinge operates on a Teflon bearing. "It would take two weeks of rock detonation in order to break through this door," Oswald remembers. All other passages require a personal code issued upon entry into the underground labyrinth. Should one attempt to enter an area without authorization, an alarm will sound. Numerous cameras survey the inner and outer areas of the property and send images of every movement to the Swissvault control center.

Artificial climate and own electricity production

During the construction and renovation of the Swiss Fort Knox bunkers, nothing was left to chance. The stored data is not only safe from non-authorized access but also from possible military and civil threats. Radioactive and electromagnetic forces are screened off, as well as impacts from natural catastrophes. "In the bunker reigns an artificial climate," Oswald explained. "No matter what happens outside, we can't feel it here inside."

In order to secure a functioning infrastructure in an emergency situation, Swiss Fort Knox is equipped with its own water reservoir and air filtering system as well as its own electricity generator. "In this way, we can rely on the high quality and constant supply of our electricity," commented Oswald. In the event of a blackout, diesel generators and whole rooms filled with batteries are ready to supply enough energy to last a few weeks.

The data is also well taken care of, even in emergencies. Every day, an automatic backup occurs taking only new and changed data from the client's computer, guaranteeing a short transfer time, regardless of a client's weak internet connection. In order to load the data back on the client's computer as quickly as possible, Swiss Fort Knox has

many specially designated telecommunication lines. For those clients who find the highly encrypted transfer over the internet too unsafe, they are given the opportunity to place their servers under the mountain and to operate them via remote control.

You can make money, but not data

The idea of a data bunker came about in 1992. After a year of planning and a year of bunker renovations, the first data services were made available in 1994.

"Until broadband internet connections became popular in 2002, our services were too expensive for smaller companies," Oswald said. "But today, small companies as well as private persons can afford data security at Swissvault." And apparently, this concept seems to have paid off. "Many companies in Saanenland are our clients," Oswald added. Local interest aside, there is a large amount of international interest. "Switzerland is commonly associated with security and reliability," said Oswald, who is convinced that this has much to do with the prestige of Switzerland as a banking center. "Depositing money and data have some similarities. The only difference is that one can always make money again if one were to lose it, but data can disappear forever."



A five-level security control protects the data bunker from physical entry: to go through the first armored door, one must be accompanied by security personnel and a security manager; the second armored door will only open once the first door is closed. A third armored door weighing 3.5 tons can only be operated by a guard. All other passages require a personal code issued upon entry into the underground labyrinth.