


DATA BACKUP

Beyond the
3-2-1 rule



In collaboration with **boolebox**

www.boolebox.com

■ A problematic context

Backing up data is one of the most common activities in the world of Information Technology. Companies do it with their employees; experts and so-called "top voices" of information technology do it with all users, from highest-level professionals to the not-so-tech-savvy ones. The suggestion is based on the common sense necessary to find one's way in a world in which cybercrime is growing exponentially. In the Clusit (Italian Association for Information Security) 2020 Report, which refers to data collected in the previous year, we learn that there were 1670 attacks in Italy: +7.6% compared to 2018 and +91.2% compared to 2014. Malware is the most widely used tool.

However, the numbers and facts do not yet allow to properly deploy a culture of backup as a basic IT security tool. There is no shortage of initiatives: just think of the institution of Backup Day, which is celebrated on 31 March each year. For the 2020 edition, Acronis released a report -2020 Cyber Protection Week Survey - in which numbers such as the following emerge:

- in 2019, 42% of companies declared data losses
- 41% report loss of productivity or money due to inaccessibility of data
- 42% again, also stated that the loss was followed by inactivity
- 85% of companies do not back up several times a day. In particular, only 15% say they do it, 26% do it once a day, 28% do it once a week, 20% do it every month and 10% do not do any backups at all
- 68% of users say they lose backups due to accidental deletion, hardware or software failure or obsolete backups; among professional users who do not perform backups, almost 50% believe it is not necessary
- only 17% of end-users and 20% of IT professionals follow best practices, with hybrid backups on local media and in the cloud.



***The
31 March
is Backup
Day***

Backup: why do it?

In view of the numbers we just mentioned, the question may appear rhetorical. But that ceases to be the case if we rely on the calculation of probabilities. Let's assume that our computer has a one in a hundred chance of breaking down, preventing us from accessing the data we store on it.

Copying and saving them on an external disk protects us from mishaps and dramatically reduces the chances of losing them. Assigning the external drive the same chance of failure as seen with the computer (one in a hundred), the calculation is simple:

$$\frac{1}{100} \text{ (computer)} \times \frac{1}{100} \text{ (external drive)} = \frac{1}{10,000}$$

We therefore have a 1 in 10,000 chance of losing our data. And if we decide to store them on another device, the probability decreases even further:

$$\frac{1}{100} \text{ (computer)} \times \frac{1}{100} \text{ (external drive)} \times \frac{1}{100} \text{ (third device)} = \frac{1}{1,000,000}$$

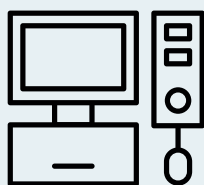
In other words, the probability of losing our data is one in a million.

The 3-2-1 rule

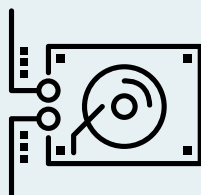
The calculation just seen expresses the rule most suggested to users by security experts, that of 3-2-1. Based on this rule, it is good to keep 3 copies of one's data: on the computer: where they're needed for daily activities; on an off-site device, such as an external hard disk; and in the cloud.

This rule is the starting point for guaranteeing the minimum level of security for one's data, and it does, of course, require certain precautions. When copying to an external hard disk, for instance, it is important that the device is not stored in the same room as the computer. The reason is intuitive: in the event of a physical accident (a fire in the room, an intrusion by thieves) both storage locations would be lost, forcing us to retrieve everything from the cloud. The latter is not a problem-free area.

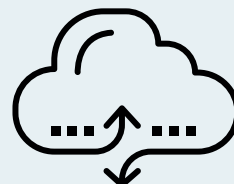
***It is wise to keep 3 copies of your data:
in the computer, in an off-site device and in the cloud***



1



2



3

■ In the cloud, data is encrypted

Speaking of the cloud as a technological novelty is now a misnomer: this storage solution is ingrained in the daily lives of millions of users. Proposed both by the so-called IT giants and by small, dynamic and highly innovative companies, the cloud branches out into many options, in fact divided into two large groups: free and paid. It goes without saying that the latter offer provides not only more space, but also a higher level of security for data storage.

But how much higher? The answer also depends on us. "An essential measure to further protect our data is not to synchronise the cloud, transferring data to it from time to time", explains Valerio Pastore, founder of BooleBox. "As Clusit and others entities involved in cybersecurity have pointed out, cybercrime and data theft are constantly on the rise", Pastore continues. "Even more so in these days of quarantine: the explosion of smart working has undermined security systems, as many workers have had to connect to company servers with their own device, which is an easier gateway for a malicious attacker to open".

A synchronised cloud would complicate an already difficult situation. "Imagine being hit by ransomware", the BooleBox founder continues. "One morning I switch on my computer and find a message informing me that my data has been hijacked: if I want to access them and the functionality of my machine again, I have to pay. If the cloud is synchronised, the ransomware is also synchronised and everything in the "cloud" is hijacked".

Does this compromise the 3-2-1 rule? "No, the rule remains valid", Pastore concludes. "For example, we might have saved our data on an external drive. But more can be done to protect them in the cloud if we forget to not synchronise them. This is enabled by a solution such as BooleBox, which encrypts every single piece of data. Even if they were stolen, that data would not be readable and would consequently not be available for use except by the legitimate owner, the only one who knows the access keys".

Data encryption, as used by BooleBox, is therefore a maximum protection solution for the "21st century oil", a phrase that more and more experts are using to refer to personal data. This reinforces the 3-2-1 rule by placing it in a different and more modern perspective of cybersecurity, which is now data-centric, leaving behind the increasingly obsolete perimeter security model.

Data encryption, used by Boolebox, is a maximum protection solution

Check out other **boolebox** white papers

Read them now

More information

Boole Server SRL

✉ info@boolebox.com

☎ +39 02 / 87 38 32 13

👉 www.boolebox.com



This whitepaper/e-book was published by Boole Server S.R.L. The usage and publication rights are exclusive to Boole Server S.R.L. No liability is assumed for any contents in this whitepaper/e-book and no guarantee is given for the correctness of the information.