ENJOY SAFER TECHNOLOGY®

THE 5 MOST COMMON REASONS FOR CORPORATE DATA LOSS

www.eset.com

The 5 most common reasons for corporate data loss

By Josep Albors, ESET Spain Communications & Lab Director

There is no doubt that one of the main assets of a company is the data it stores. Information about its customers, financial or employee planning, among other types of records, should be adequately protected and available whenever they are needed. For this reason, companies that care about such data invest adequate resources into protecting them and recovering them in the event of a serious incident.

But how serious does an incident need to be for vitally important stored data to be lost? A recent study by *Kroll Ontrack* revealed very interesting data gathered using the company's data recovery tool.

Let's look at the main reasons for the loss or leakage of corporate data. Below is the complete list, together with the proportion of cases for each reason:

Cause of data loss	Percentage of respondents
Undetected drives	**25%**
Not powering on	**11%**
Device dropped from height	**10%**
Deleted files	**9%**
Corruption	**7%**

Hardware failures

According to the study, the main problem, accounting for 25 percent of the total number of cases, is failure to detect the storage drive. That is logical, especially if we are talking about hard drives and flash drives, which are used in mass storage devices in all kinds of corporate environments despite being much more prone to failure than other more reliable types of devices, like magnetic tape.

Furthermore, the increased use of solid-state drives (SSD) with flash memory in recent years will undoubtedly have pushed this percentage up. These types of drive offer faster access to data than conventional mechanical hard drives, but also are more prone to failure if used to write

data continually, which is why they are not recommended for use in servers or in computers where reliability is critical.

Another of the big problems behind data loss is the device not powering on, which can be caused by a failure in the power supply or in other components. Curiously, in third place, we find one of the reasons that can cause hardware to fail—the device being dropped.

We should bear in mind that normally such hardware failures don't necessarily have to result in irreparable loss of data, as it can usually be recovered by using forensic analysis tools or even, in cases where the device has been damaged but the disk itself still works, by placing the disk in a new device.

Software failures

In fourth and fifth place in the table, we find two reasons that tend to be caused by software failures occurring at the same time as the data is being used, or malware that directly affects the stored data. So here we are talking about files being deleted (accidentally or deliberately) or becoming corrupted.

Both of these reasons can be caused by the user making a bad decision or by a system failure, but in recent months we have seen how ransomware has become a major threat to corporate environments. Its malicious actions can include the two causes of data loss mentioned above.

To better understand ransomware and how to protect your files and data, *download this free guide* to ransomware security.

Data corruption is self-evident, given that ransomware encrypts the files, making them inaccessible unless they are decrypted, and in order to do that the cybercriminals demand a ransom, which may be large or small. It goes without saying that we do not advise paying such ransoms, because by doing so we would be giving these criminals more of an incentive to keep creating new similar threats.

As for data deletion, we have recently seen cases of malware like *Jigsaw*, which deletes a certain quantity of files every so often if the victim does not yield to its demands, and deletes even more files if he or she tries to restart the system.

The importance of prevention

Faced with such incidents, which can put companies in a serious predicament if they do not respond in the right way, the best solution is prevention and having sufficient measures in place to recover the affected data as quickly as possible, so that the company can keep its operations running normally.

This includes things like security measures provided by an *antivirus solution* to prevent the kinds of damage that malware can cause. *ESET Endpoint Security*, for example, is equipped with proactive malware defense and engineered to be light on your systems, delivering protection across endpoints and increasing end-user efficiency without slowing down computers.

For hardware failures, the best thing is to have a *backup system* that can quickly restore not only the data stored but also the system on which they are stored, thus minimizing the response time and enabling the company to keep operating normally. ESET offers the easy-to-use, flexible software *StorageCraft* as our backup and recovery software solution.

Bear in mind that the results of this type of incident can be irreparable, so it is best to be prepared so you can respond adequately if and when it happens.

Want to learn how to mitigate risk at every angle? Read how to perform a security audit in our new tech brief, "*Security Audits: What is your game plan?*"

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®