

Ensuring Security

2 tokens, double the security



Recent reports of company-compiled personal data gone missing, while clearly catastrophic, are just the tip of the iceberg. What customers really need to ask of companies is, what other data has been lost? In all likelihood, there is absolutely no way for companies to know.

The truth of the matter is reported cases of massive data loss are just the ones they know about. This problem will only grow with the proliferation of tiny personal mass-storage devices of dramatically increasing capacity.

How many people currently own flash memory drives? Tens of millions. And how many companies actually control the use of flash drives? You can count them on one hand. I travel a lot and on a recent trek, I happen to stumble onto a flash drive fallen under the table through a custom security check in the airport. This lost drive has no distinguishing characteristics – no label to indicate the owner or where he worked. With some time to kill before my flight, I decided to see if I could track down the owner. Unfortunately, that requires me to intrude the owner's privacy. Turns out that the files contained fairly innocuous content – some project plans and a short PowerPoint in draft form- but no way to identify the owner.

Why is this an issue? Commonly used portable devices include external hard disks, tape backups etc. These commonly used devices' capacities have increased tremendously in a short period of them. With this improvement, more data that are possibly not encrypted are stored on such devices that are obviously scattered

and disorganised. And this is evidently a huge risk that corporates have to undertake if their users are using these devices as the information stored in these devices may be confidential and critical to the company. The potential to lose data on portable devices is a massive hole in many companies' security plans. Majority of such devices are possibly not encrypted or safe guarded..

REDiSAFE's two token security key ensures security to all data stored in its server. It allows the data to be encrypted and prevents invasion of data both externally and internally. The admin token, used for encrypting the data acts as a preventive measure to ensure maximum security even if your server is stolen. Without this key, data stored on the REDiSAFE server cannot even be accessed.

“The potential to lose data on portable devices is a massive hole in many companies' security plans”

The emergency token on the other hand acts as a key that allows emergency recovery to the accounts and allows highly confidential data to be access only by the rightful users. In most cases, this key is managed by its highest appointment holder in the company to ensure that internal security is not jeopardized and breached.

Even up to today, not all data security problems have been resolved”. With REDiSAFE, however, we can close that security gap and help employees to understand and be aware of the importances of data security, easing them with functionality and convenience for data protection.

Text by Justin Foo