给金融类公司设计软硬件架构，几乎每星期都会被问这种问题。包括但不限于：

如何不让程序员删库？

如何不让非授权人员接触数据？

如何在物理服务器损坏的情况下保护数据？

如何在整个数据中心损坏的情况下保护数据？

如何在备份数据中心也损坏的情况下保护数据？（一般客户问这个问题，我都会反嘲一句，相隔100公里以上两个数据中心同时损坏，这时候你们还要上班嘛）

在行业内，数据恢复，有两个指标，RPO，RTO 这两个指标是区分爱好者和行内的第一层过滤。

RPO 是指系统恢复时间点，RTO 是指系统需要恢复的时间。打个比方， RPO 24 小时，RTO 3 小时，也就是当系统宕机以后，3 小时内可以恢

复到 24 小时以前的数据。

RPO 和 RTO 越优，备份策略越强，价格成指数上升。我曾经为一个银行做过 RPO 0，RTO 0.5 小时的设计，硬件加中间件就上千万，还不算机房房价。

中小企业，尤其是 50 人以下的公司，事实上是承担不起这种典型的正规设计的。所以一般来说，中小企业都建议使用云解决方案，个体物理方案，中小企业是有成本限制而无法达到的。

>>> 脚本不传播，尤其是含有删除命令的脚本。