It is no secret that Google has world-class data centers and disaster-recovery capabilities. But what you may not know is that Google's disaster recovery capabilities are designed to protect Google from disasters that affect them, but not necessarily to protect you from your own business disasters.

One third of all data loss is just plain old user error, and Google can't protect you from it.

Moreover, as the cloud encourages collaboration, the risk of user error only increases as a growing number of users share access to an ever increasing percentage of your important business data.
An emerging type of cloud data loss is corruption and deletion caused by third-party applications. When you install add-ons to cloud applications like Gmail, Google Docs, and Google Apps, you increase the potential for a software bug to wreak havoc on your business data. Similarly, as you expand the number and types of devices that can access your data, you expand the number of platforms that can invoke these third-party applications. Put more simply, tablet and smartphone apps can access your Google Apps data, but they often lack the rigorous quality controls associated with traditional PC software. For example, there are many reported cases where mobile device apps that were meant to synchronize calendars and contacts instead deleted all the calendars and contacts for a given user.
Another major concern for cloud data is hacked accounts, which typically follow one of two main forms. In the first case, an intruder deletes all a user's data as a precursor to employing the account in a spam attack. The second typical form of hacker-related data loss is malicious deletion, wherein an account user – often the primary account owner – simply deletes data without knowing what the consequences are upon synchronization. Google's disaster recovery capabilities simply aren't designed to respond to this granular level of data loss. Google has no way of distinguishing between legitimate deletions and deletions caused by attackers who have somehow gained apparently "authorized" access.
Consider the case of a Google Apps customer who recently found himself in a dispute over amendments to a contract, where both parties had agreed that an email communication would serve as the documentation of a contract change. He was unable to find the email in his Google Apps account, and didn't know why it vanished, so he had no proof of the contract changes – or the agreed upon fees associated with the change in terms.

NETCOM HOSTED MICROSOFT EXCHANGE 2013 ADVANCED ACCOUNTS INCLUDE ACTIVSYNC, ARCHIVING AND RETENTION AS STANDARD CORE SECURITY FEATURES.