How To Avoid Data Catastrophe

Matthew O'Keefe
Forbes, Feb 26, 2019,

Human nature has inherent biases that can disable our ability to make the right decisions in both simple and complex environments, including business ones.

Research has shown that multiple near misses foreshadow almost all disasters and business crises, but most of those incidents are ignored or misread. Two cognitive biases in particular cloud judgment in those cases.

Getty Images/iStockphoto

One is called “normalization of deviation,” the tendency to accept as normal deviations from correct behavior. Consider texting while driving. Research shows it impairs driving ability nearly as much as consuming alcohol, yet drivers not only continue to do it, but they also feel more confident it is safe the more times they text and drive without incident.

Within a large organization, this normalization can potentially cause a catastrophe. Diane Vaughan coined the phrase “normalization of deviation” in her book *The Challenger Launch Decision* about the first space shuttle disaster.

The second catastrophic space shuttle accident, with Columbia in 2003, provides a prime example of a second cognitive bias, known as “outcome bias.” Foam insulation

falling from the external fuel tank damaged Columbia's wing during liftoff, resulting in the shuttle's complete disintegration at re-entry. Dozens of missions had been flown successfully even with these foam strikes, so NASA had reclassified those events from near misses to maintenance issues.

Outcome bias leads even experts to focus on a successful outcome (or series of outcomes) rather than the complex processes that lead to success, even when near misses are indicating that the underlying processes have flaws.

Data Protection Bias

Normalization of deviation and outcome biases are also common in the data protection cultures of most enterprises, including multibillion-dollar corporations, sometimes putting priceless data at risk.

Many companies keep their most important data in an Oracle Database, yet they often tolerate or don't detect their failed data protection and backup methods. False signals indicating a successful outcome are common.

Two personal experiences provide some perspective on this problem.

I once attended a meeting with database backup administrators at a very large insurance company. The admins insisted that none of their backups had ever failed, yet members of the infrastructure team that supported them had told me that they failed all the time. There was no consistent process to test recovery for all backups, so successful recovery was simply assumed if a backup was successful—a classic case of redefining deviation as normal and being lucky that no recovery requested actually failed.

In another case, one of the largest US companies started evaluating a product (Oracle Zero Data Loss Recovery Appliance, or ZDLRA), which indicated during a test that data generated by the production backup process was not recoverable. The company's existing production system, in contrast, indicated the backup was successful. Turns out that ZDLRA showed that the production system had a near miss that was avoided only because that incorrect data was not required for an actual recovery. If it had been, a catastrophic loss of data would have occurred, possibly resulting in downtime, regulatory fines, and loss of business.

Critical Management Skills

Time and cost pressures add to the likelihood that design failures will either be tolerated or go undetected. Time pressures also lead to decision-making based on rules of thumb or gut instincts rather than refined processes.

To avoid those traps, it's important to learn from deviations, uncover root causes, and demand accountability.

Another critical management skill is to envision worst-case scenarios. In one survey, people were asked if they would evacuate from a hurricane given a 30% chance of their homes being hit. If told that their house had escaped damage during previous hurricanes, survey respondents were likely to stay put. However, if told that a neighbor's house had been destroyed by a falling tree during a previous hurricane (i.e., they were prompted to visualize a worst-case scenario), respondents were much more likely to evacuate.

As for the data protection and recovery process, chief information security officers and chief data officers must insist on regular reviews, encouraging and even rewarding staff to report failures so that they can be addressed in the open.