the Availability Digest

www.availabilitydigest.com
@availabilitydig

Human Triple Whammy – NYSE, UA, WSJ

July 2015

IT outage statistics show that about 40% of all system outages are caused by humans and that approximately 70% include humans in one way or another. Human frailties combined on Wednesday, July 8, 2015, to take down three major systems – the New York Stock Exchange, United Airlines, and the Wall Street Journal.

These outages emphasize the point that redundancy should apply to humans as well as systems. Any human action that represents a single point of failure ought to be undertaken by a team of at least two people, one proposing and performing the action and another checking and approving it.

New York Stock Exchange

In the early hours of Wednesday, July 8th, technicians at the New York Stock Exchange (NYSE) were busily upgrading the software to its gateways to support an upcoming change to the Session Initiation Protocol (SIP). SIP is a communication protocol for controlling multimedia communication sessions, typically Internet voice and video and instant messaging over IP.

During final testing, around 7:30 AM local time, problems were discovered with the update. The gateways were misconfigured for the new software release, causing communication issues between the customer gateways providing access between the member brokers and the NYSE trading systems. The gateways were reloaded with the proper software version, and the markets opened on time at 9:30 AM.

However, as the morning progressed, additional communication issues between the gateways and the trading systems emerged. They became so severe that trading was shut down at 11:32 AM. In a statement, an NYSE spokesperson explained, “It was determined that the NYSE and NYSE MKT gateways were not loaded with the proper configuration compatible with the new release.” It was not feasible to simply back out the upgrade and continue on with the original known configuration since this might have caused many trades to be canceled.

The termination of trading by one of the most important stock exchanges in the world is a disastrous event. On an average day, the NYSE executes about four million trades worth about USD $50 billion. If trading stops, customers cannot buy and sell shares; and brokerage firms lose millions of dollars in commissions.

The NYSE faced a particularly difficult deadline in that mutual funds and other investment vehicles need a closing price in order to evaluate their portfolios, a regulatory requirement. As the 4 PM closing bell approached, things grew tenser.

Finally, at 3:10 PM, the NYSE was able to get its trading systems operational, and trading continued at a frenzied pace until the 4 PM close. The stock exchange had been down for nearly four hours.

The NYSE outage was definitely caused by a human manual configuration error. Not only was the update poorly planned, but the testing of the upgrade was insufficient.

United Airlines

On the same day as the NYSE outage, July 8, 2015, United Airlines (UA) lost its reservation system for 90 minutes in the morning, U.S. time. It had to cancel 59 flights, and over 800 flights were delayed around the world. Passenger agents frantically tried manually to issue boarding passes and to rebook passengers but were unable to make a dent in the lines of passengers frantically trying to get onto flights.

United blamed the outage on faulty network connectivity caused by a router malfunction, which disrupted its reservation system and degraded network connectivity for various other applications.

United has experienced several IT problems since it first merged its computer systems with those of Continental Airlines, which it acquired in 2010. Experts point out that this resulted in a massive interconnected complex of patched computer systems that has proven difficult to manage. They claim that United has not supported its IT infrastructure with sufficient staffing, testing, and backup systems.

The United failure was caused by a failed router. Was this a human failure? It is apparent that United's interconnection network probably does not have pervasive redundancy or monitoring facilities to rapidly detect and isolate problems. With effective redundancy, the failed router should have been replaced automatically with a backup in seconds. Proper monitoring would have alerted IT staff immediately to the problem so that they could take further steps if necessary.

Why was there insufficient redundancy and monitoring? Probably financial considerations. Decisions by humans.

Wall Street Journal

Adding to the excitement of the morning of July 8th (and to the delight, I'm sure, of its competitors), a third major company faced problems. Just before noon in New York City, the web site of the Wall Street Journal (WSJ) started responding to user requests with 504 (timeout) errors. The problem became so severe that the web site was effectively nonresponsive to most requests.

The problem happened just minutes after the NYSE shut down at 11:32 AM, leading most people to conclude that the web site succumbed to an overwhelming request for explanations as to why the NYSE had stopped trading.

This fault was caused by a web site implemented with insufficient capacity and without the capability to burst excessive traffic to a cloud. Whose fault was this? Management. Again, the finger for this failure can be pointed to the human.

Summary

At first, many were convinced that these failures were the result of a massive coordinated hacking attack. Just the previous evening, the Anonymous hacking group had tweeted "Wonder if tomorrow is going to be bad for Wall Street … we can only hope." However, the detailed descriptions of the faults put this speculation to rest.

Human beings have their fingers into most causes of IT failures, whether it be an overt action like typing the wrong command or a management decision that leaves IT systems vulnerable. When it comes to the use of IT staff, there are several things to consider:

- If there is an operation that must be accomplished manually and that will cause a system failure if performed erroneously, use two people, one to propose and execute the operation and the other

to approve and monitor it. Operations such as this range from entering a sensitive command to pulling a failed board rather than the operational board.

- Failover to a backup system is one of the most difficult operations to perform successfully. Failover faults all too often prevent the recovery of a failed primary system. Many failover faults are caused by human errors. Failover procedures should be highly automated, and any remaining manual procedures should be fully documented. The failover process should be practiced periodically to make sure that the procedures are correct and that the people are properly trained.

- All software changes should be reviewed by one or more qualified people. This is another example of human redundancy. A software error would have to be missed by two or more people.

- Any upgrade to a system must have associated with it a planned backout procedure to return to the known working configuration. Upgrades are implemented by people. People make errors.

- Management must ensure that the resources required for adequate staffing, testing, and redundancy configurations are made available to the IT department.

Acknowledgements

Material for this article was taken from the following resources:

United Airlines, NYSE Outages Reveal Poor Redundancy Architecture, Insufficient Testing, *CRN*; July 8, 2015.
United Airlines blames grounding of hundreds of flights on computer glitch, *LA Times*; July 8, 2015.
Oops, 504!, *Politico*; July 8, 2015.
NYSE outage highlights need for IT automation, *Search Data Center*; July 9, 2015.