Trading Sector Parses Knight Breakdown
August 2, 2012

The technological glitch that caused Knight Capital to lose $440 million through erroneous trades on Wednesday morning has passed, but analysis of the disruption is only beginning.

Coming on the heels of a host of other recent financial-market woes – spanning an array of names such as JPMorgan, Nasdaq, Facebook, Bats, Barclays, Peregrine, and MF Global – the Knight breakdown arguably has come under extra scrutiny.

Knight, an electronic market maker based in Jersey city, New Jersey, has said Wednesday's trading debacle, which caused erroneous trades in about 140 stocks, stemmed from an installation of new trading software. As was the case in the much broader 'flash crash' of May 6, 2010, market participants noted that the high-speed nature of trading may not have caused the problem, but it at least fed into the problem after it started.

"The rapid implementation of automated execution algos has skewed the markets from a point of relative balance to an overstretched position that carries significant tail risk," said Karim Taleb, principal at investment manager Robust Methods. "The cost of otherwise small technical glitches has become disproportionately large hence, and constitutes a significant financial risk for investors and the capital markets."

"The Knight situation is a warning flag pointing to an overly permissive market microstructure which cannot absorb small technical issues, and highlights a pressing need for restoring price quality and market robustness," Taleb told Markets Media.

Flexible and configurable algorithms and software are less risky than "hard-coded" mechanisms, according to Cyborg Trading Systems.

"The lesson (of Knight) is a reaffirmation of the importance behind multi-layered risk monitoring and system control," said James McInnes, chief executive of Cyborg. "It is important to have independent risk controls at the algo level, product level and account level."

"At the very core of mission-critical software is the concept of fault intolerance," McInnes continued. "This means that the system will shut down if some operating characteristic exceeds its nominal performance envelope. External fail-over mechanisms may then be tripped, but the flawed system is no longer allowed to continue operation."

Consistent pre- and post-trade risk controls to limit the number of filled contracts and monitoring order-flow profiles can help prevent future trading snafus, according to Steve Woodyatt, chief executive of trading-services firm Object Trading. Additionally, basic trading-system stop-loss protections would limit the damage of a continuously errant system crossing the spread.

"Machines only do what the human trading-system developer tells it to do, which appears to be, in this case, to cross the spread," Woodyatt said.

Added Taleb, "the lesson is that the current market microstructure needs to be tightened somewhat by including minimum quotations resting times and minimum order execution time-buffers to limit and slow down any damage that would result from future glitches."