CITS5501 Software Testing and Quality Assurance
Risk case study – Knight Capital

Unit coordinator: Arran Stewart

Overview

- Adapted from post by Henrico Dolfing
- Knight Capital Group was an American global financial services firm engaging in institutional sales and trading.
- In 2012 Knight was the largest trader in U.S. equities with a market share of around 17 percent on the New York Stock Exchange (NYSE)
- Knight's Electronic Trading Group (ETG) managed an average daily trading volume of more than $21 billion daily.

2012 Loss

- On the morning of 1st August 1, 2012, new trading software was activated when the NYSE opened that day
- It contained a flaw that only became apparent at that point
- In the space of an hour, the software started repeatedly bying stocks worth $7 billion

What had happened?

- Knight Capital wanted to participate in a new market the NYSE offered, but would need to develop or adapt trading software for the market in only 30 days.
- Knight Capital adapted old code from their “order router”, SMAR (Smart Market Access Routing System)
- SMARTS contained unused (“dead” code), previously used for a test program that made deliberately bad trades (bought high and sold low), and was only supposed to be used in a test environment

What had happened?

- Knight Capital had made significant code changes to SMARS over thre years, without thorough regression testing
- The week before the software was to go live, the new software was manually (not automatically) deployed to eight servers.
- However, the engineer doing so made a mistake and did not copy the new code to one of the servers.

The crash

- At 9.30 am on 1st August 1, Knight began receiving orders from brokers, and SMARS distributed the incoming work to its servers.
- The seven servers with new code processed the orders correctly, but the eighth server began to continuously send orders, without regard to how many had already been performed
- This resulted in 4 million executions in 154 stocks for more than 397 million shares in approximately 45 minutes.

Steps to fix

- Although the system emitted diagnostic alerts, these weren't acted on, and the problem was only realised by external analysts who traced high-volume trading back to Knight and informed the CIO at 9.34 am
- However, Knight had no documented procedures for incident response, and it wasn't until 9.58 am that engineers worked out the cause and shut down SMARS.

Possible preventative measures

- What problems can you see here?
- What could Knight have done differently to prevent the loss?