

Operational risk

Eliminating harmful spreadsheet risk

Spreadsheet errors can cost a firm millions and some banks are still vulnerable – but there are solutions around

In 2003 Canadian power company TransAlta Corp took a \$24 million charge to earnings after a bidding mistake resulted in it buying more US power transmission hedging contracts than it required, at higher prices than it wanted. The company's computer spreadsheet contained mismatched bids for the contracts. TransAlta chief executive Steve Snyder said "it was literally a cut-and-paste error in an Excel spreadsheet that we didn't detect when we did our final sorting and ranking of bids prior to submission".

"The problem with spreadsheets is that they are generally built by non-programmers", says Yusuf Jafry, chief technology officer and co-founder of finance and risk management software firm Risk Integrated, which is based in Douglas, Isle of Man, the UK Crown dependency, and in Garrison, New York.

Spreadsheet risk is the danger that errors in a common business tool such as Microsoft Excel can cause material losses when used inappropriately by financial organisations.

Errors creep into formulas, some from formatting and some from links to other spreadsheets. Most are due to negligence, although a few are due to fraud.

"There are no thorough procedures in place to check the accuracy of the spreadsheets, or to test multiple runs of data through them," says Jafry.

Rules put in place

Today most banks already have established sets of rules, standards, and controls over their accounting systems and many of the databases they access. But Jafry says controls have not been put in place for their smaller systems, such as spreadsheets, although some firms are now addressing the problem in response to the Sarbanes-Oxley corporate governance laws in the US and the operational risk requirements of the international Basel II bank capital adequacy rules.

"The financial software industry has responded in a number of ways. There are various spreadsheet auditing tools

available that can help to build reliable spreadsheets, and there are tools available to help end-users build new, robust spreadsheets from scratch", says Jafry.

More comprehensive spreadsheets are beginning to emerge in the market place. These so-called business intelligence, or BI platforms, aim at providing a set of common services to help integrate information and data sources.

According to media reports, Microsoft is working on a BI solution to accompany the release of the next version of its Excel spreadsheet, scheduled for 2007.

Jafry says Risk Integrated has its own product – Enterprise Spreadsheet Platform, or ESP. The aim with ESP is to provide spreadsheet management under which the spreadsheets are exposed only to a few designated experts, or superusers, in an organisation.

The objective is the near elimination of spreadsheet risk, while maintaining the full flexibility of spreadsheets for modelling complex financial structures and processes.

The superusers are responsible for maintaining the integrity of the spreadsheet models, and for "uploading" their tested and "signed-off" versions to a centralised server or database. ESP has tools that monitor, assign and track changes to the spreadsheets. A full audit trail can track the versions of spreadsheet models against users making the changes. **GRR**

The classic case – Allied Irish

The classic case of fraudulent manipulation of spreadsheets occurred at Allfirst Bank, US subsidiary of Allied Irish Banks where rogue trader John Rusnak was discovered in 2002 to have lost \$691 million through unauthorised currency trading.

The case illustrates the point that one error in a spreadsheet will subvert all the controls in all the systems feeding into it, according to Ray Butler, co-founder of the European Spreadsheet Risks Interest Group (EuSpRIG), a group of academics and industry people that promotes research into spreadsheet risks.

Rusnak manipulated the principal measure used by Allfirst and AIB to monitor his trading – value-at-risk, or VaR – by directly manipulating the inputs into the calculation of VaR used by an employee. The employee was supposed to check the VaR, an estimate of the maximum range of loss likely to be suffered in a given portfolio, independently. But she relied on a spreadsheet that got information from Rusnak's personal computer that included figures for so-called handover transactions which were entered into after a certain hour toward the end of each day. But the transactions weren't real and weren't entered on the bank's trading

software. They were simply a way to manipulate the spreadsheet used to calculate the VaR. A simple check to see if the holdover figures were captured in the next day's trading activity would have exposed the scheme.

Currency rates were also downloaded from Rusnak's Reuters terminal to his personal computer's hard disk drive, and then fed into a database accessible to the front, middle and back offices.

Butler, in a paper available on the EuSpRIG website (www.eusprig.org), says the lessons for audit and control of spreadsheets are:

- Be alert for the possibility of deliberate manipulation of spreadsheets, as well as innocent mistakes.
- Ensure all important spreadsheets are risk assessed and tested where appropriate.
- Ensure key data items and constants are checked to source and critically reviewed – the calculations in the VaR model were correct, Rusnak interfered with the data.
- Existing software, such as SpACE, would have highlighted the presence of the links in the pricing spreadsheet, and explained where they went, to enable follow up early in the audit process.
- When potential weaknesses or risks in a system are detected, follow them up