A Crisis of Confidence

By Scott M. Shemwell

In a climate where the financial markets turn a skeptical eye toward company financials, it behooves the energy trading industry to make systems as bulletproof as possible so as to avoid any hint of scandal.

At 5:03 a.m. Monday the phone rings and wakes you up to an alarmed CEO on the other end. Your largest European and U.S. competitors have just terminated their joint venture and announced liquidation of some assets to meet loan covenants. On the Financial Times Stock Exchange these stocks have plummeted more than 30% each.

At 6:57 a.m., your meeting with the executive committee convenes. The New York Stock Exchange opens in a little more than two hours and already analysts are calling. Does your firm have a liquidity problem? At the bell, your stock along with that of all your competitors' opens 5% lower. There's nothing you can do about the markets, you muse, and as CIO go about your business managing the firm's information systems.

At 11:56 a.m., your director of information technology (IT) tells you the company's central trading system has just been hit by a denial of service. The system is locked and will stay that way for at least an hour. At 12:04 p.m., the vice president of trading is on the phone: one of your largest accounts cannot transact business and is threatening to go to the competition. At 12:12 p.m. the CEO calls and says one of the analysts heard a rumor that your company had stopped trading energy commodities. At 12:17 p.m., your stock is down 25 % on a false rumor that your company lost $10 million on one transaction.

A stroke of luck brings the system back to normal by 12:22 p.m. but not before a disgruntled ex-employee has informed an Internet chat room that hackers have sabotaged your computer systems and stolen critical customer records. The ex-employee and the instigator of the denial of service are one in the same and the FBI arrests him 48 hours later.

Two trading days later, your stock price is still down by

17% as the market continues to digest the events and looks for assurances that this will never happen again.

Nightmare scenario? Perhaps. Unrealistic? No. A recent front page *Wall Street Journal* article covered the devastating impact on a restaurant that was wrongfully accused over the Internet. It has happened and it probably will happen again—even in the restaurant business.

If anything, the markets might react more negatively to this crisis of confidence. Unplanned downtime happens. Often it is seen as no big deal. A throwback to the back-office offline, MIS mentality, many executives are unaware of the impact real-time trading systems can have on a firm's shareholder equity. Moreover, we can expect security issues to remain at the forefront of management concerns.

Businesses grounded in solid economic theory are more likely to prosper in an uncertain world. Modeling can predict behavior, and when data is scrutinized for decision support, the inherent descriptive limitations of stochastic analysis create boundaries. In a changing environment, exchanges should be founded on business fundamentals and core ethical values.

Many executives are unaware *of the impact real-time trading systems can have on a firm's shareholder equity.*

THEORETICAL CONSTRUCT

Modern energy trading firms effectively integrate portfolio management theory and real options theory. The integration of these two economic theories at their equilibrium margin is internally consistent in that financial theory argues that portfolios are established to mitigate risk across a set of investments and real-options approach extends the option-pricing theory for managing a set of real assets. In other words, the firm strives to achieve a set of investments or projects that lie on the economic efficiency frontier, or a portfolio of investments that have the highest expected returns at an indifferent standard deviation or level of deviations from the probable. Standard deviation is the statistical measure of deviation from a norm or level of risk that the norm will not be achieved. Investments with a large standard deviation are, by definition, more risky than those with a smaller standard deviation.

Like much of traditional economic theory, portfolio management has its roots in John Maynard Keynes' "General Theory of Employment, Interest and Money," first published in 1936. Since then, organizations have embraced Keynesian economics and managed their portfolios as a function of the implied equilibrium of the statistical risk-reward curve; higher risk has economically expected higher returns, although the downside is greater. Lower risk scenarios will return reduced, albeit theoretically more consistent, earnings and cash flow.

The investments will vary in their return potential. However, the overall portfolio can be expected to add maximum shareholder value at the economic efficiency frontier. That is, no other portfolio has a higher return at the same or lower standard deviation or same yield at a lower standard deviation. This suggests that if the current portfolio is not efficient, management can increase the expected return without incurring additional risk.

Real option theory has its basis in the Nobel Prize-winning work of three economists. Commonly referred to as the Black-Scholes Option Model, this construct provides a precise model for determining the equilibrium value of an option. Asset-based energy traders establish the value of their financial option instruments against their portfolio of physical delivery options—whose value exceed that of their derivative financial instruments.

These two theories integrate at their marginal efficiency frontiers. Together they provide the asset-based energy trader with powerful tools to manage a forward-looking business.

These financially driven trading models, as opposed to asset operation, are heavily dependent on two fundamental commodities. Access to the capital markets and their inherent liquidity is key to the trading process. Equally important, timely, accurate and valid information is critical to optimizing the organization's portfolio on the efficiency frontier.

Many trading firms presently are altering their capital structure. The capital markets are requiring that firms document a strong balance sheet and in many cases this requires paring down accumulated debt. One approach has been to sell certain assets. When required to sell assets into a weak market, shareholder value is negatively impacted.

Many energy traders are facing a crisis of confidence that may or may not be deserved. However, the industry is being painted with the same brush used on the weaker firms. To secure access to capital markets and maintain customer confidence, industry players must show that their financial house is in order and that their trading systems are up to the task.

ROLE OF INFORMATION

Trading is an information-centric process. The value of a commodity is a function of its supply and demand—classic economic equilibrium. Moreover, the spot price is a function of the sum total of imperfect information available at any given time and the market's discounted perception of its future. Likewise, the future price curve is determined by the market's perception based on available information. Trading systems are information dependent engines

consisting of two components: the trading and settlement process itself and the decision support system feeding traders "real-time" information.

It is appropriate to describe these systems as real-time operations, if real time is defined to mean that the information systems provide data and information within the time constraints that are acceptable for a given decision. For example, weather forecasts are not to be updated as often as commodity market information or current political and economic news.

Successful trading organizations establish and police corporate policies and procedures that are designed to ensure that actions undertaken by employees who work on the trading floor and supporting back offices are both ethical and legal. Likewise, organizations must put in place information management policies and procedures that ensure information is properly protected and managed.

Energy traders have a wide variety of information to manage, e.g., customer data and contractual agreements, as well as active and historical trading activity. These data are critical to the firm and must be appropriately protected.

CRITICAL INFORMATION SYSTEMS

This industry is currently restructuring itself. The market and customers have concerns over the energy trader's abilities to fulfill contracts as economically viable entities. According to Glen Grabelsky, senior director of credit policy for Fitch Inc., "if there is a bar that has been raised, the investors and the marketplace have raised the bar. There is a crisis of confidence that is keeping the companies from the capital markets."

Energy traders are wrestling with a difficult situation, but they cannot overlook one other pillar that must be grounded in bedrock. The information systems that drive revenue-producing processes must be robust systems. Often overlooked, these systems are the critical underpinning of the trading process. Failure of these systems at critical moments can lead to serious economic loss. However, management often views these systems as IT issues and delegates responsibility to others.

Management cannot delegate the accountability for computer systems that are critical to the shareholder value. There is precedent for this, as previously the Securities and Exchange Commission charged publicly traded firms with the fiduciary responsibility of assuring investors that potential Y2K issues and their potential impact on operations were adequately mitigated.

Organizations must put systems in place that are scalable, secure and fit for purpose in the energy tradingenergy-trading environment. These systems must be built upon a solid data management foundation that transcends the application suite regardless of vendor and provides physical, as well as logical security.

Global reach, reduced costs and improved services are some of the important motivating factors for organizations to conduct business via the Internet. Benefits to consumers appear in the form of convenience and faster access to information, goods and services. However, conducting business on the Internet poses several reliability and security challenges.

RELIABILITY

Data management systems can now be designed to eliminate the need for planned downtime and withstand any failure: system failure, storage failure, site failure or human error. Even if hardware, such as a server, fails, online revenue generating applications must remain functioning. Today's systems accomplish this seemingly impossible task by:

- Increasing insuring fault tolerance from system failures.
- Protecting data from site failure and storage failure.
- Identifying and quickly resolving human errors.
- Eliminating the need for planned downtime.

The other important data management requirement is timely availability. Energy firms' global operations are online 24/7. Traders throughout the world need to access a single instance of data. Gone are the days of replicating or mirroring data across myriad database systems. Modern firms collaborate in real time from a single logical database or instance.

This distinction is important because in the rapidly changing trading environment, traders in offices throughout the world need access to the current situation. Previous data handling techniques had a built-in latency or delay across the different data instances.

SECURITY

Security has always been critical to the trading environment. In light of the events of the fall of 2001, it has become even more essential. IT systems can fail and sometimes do. Events such as Houston's flood in the summer of 2001 damaged or destroyed a great deal of data collected through years of research in the Houston Medical Center, arguably one of the most important medical research facilities in the world. Some data lost was truly irreplaceable; the effects of which will be felt for years.

Most readers are familiar with virus attacks perpetrated through e-mail. Less well-known are attacks such as denial of service where the perpetrator harnesses a network of online systems to effectively overwhelm the server under attack. Cyber security will continue to be a critical issue, as hackers continue to perfect their nefarious art. And firms will continue to be accountable for the protection of critical data.

Data must be secured physically as well as logically and electronically. ■

Scott Shemwell *is vice president for Oracle Corp. He can be reached at* 713.750.4046; scott.shemwell@oracle.com.