It's a lethal combination of process oversights and system failures that is the stuff of CIO nightmares: An investigation into rogue trader Jérôme Kerviel's allegedly fraudulent actions at Société Générale bank uncovered an apparent breakdown in financial and internal IT controls subverted by an employee with IT know-how and authorized systems access.

The tale of Kerviel's exploits, which led to $7.2 billion in losses for one of France's largest banks, continues to unfold as French police probe the 31-year-old trader's transactions. On April 18, Société Générale named its former CFO, Frédéric Oudea, as CEO, replacing Daniel Bouton, who remains the bank's chairman. The company is also rumored to be a takeover target.

Meanwhile, IT experts say, the case should serve as a warning that businesses can do better to manage IT-related risk.

"Much time is spent on protecting the external threat," says J.R. Reagan, managing director and global solution leader for risk, compliance and security at BearingPoint. "But the internal threat can be even larger in terms of risk to the company." In the case of Société Générale, not only were IT security controls insufficient, but the bank's staff did not fully investigate red flags that arose. Recent research by the Ponemon Institute concludes that "insider threats represent one of the most significant information security risks." In a survey of 700 IT practitioners published by the group in February, 78 percent said they believe individuals have too much access to information that isn't pertinent to their jobs, while 59 percent said such access presents business risks. What's more, IT professionals see a disconnect with business leaders: 74 percent said senior management does not view governance of access to information as a strategic issue.

Many business executives don't know what their risks are and, even if they do, they may have a tough time balancing potential losses against potential gains, says Scott Crawford, a security expert and research director at Enterprise Management Associates. "There's always this delicate balancing act between taking advantage of opportunities and doing an effective job of IT risk management," he notes. "This notion of business risk exposure in IT still is a challenge particularly for the CIO but for the business as a whole."

The Société Générale case offers lessons for IT leaders in how to manage access-related risks.

**Exploiting a Risky Business**

One of Société Générale's primary business lines is derivatives—financial instruments that allow traders to make contracts on a wide range of assets (such as equities, bonds or commodities) and attempts to reduce (or hedge) the financial risk for one party in the deal. Trading derivatives, however, necessitates some aggressiveness and can be fraught with risk. (Think of the infamous story of Nick Leeson, a former derivatives trader whose unauthorized speculative trading led to the collapse of the United Kingdom's Barings Bank in 1995.)

The French bank isn't the only company recently to suffer from risky behavior by employees. Bear Stearns, rocked by losses from its investments in subprime mortgages, was acquired by J.P. Morgan Chase for $2 a share in March when clients lost confidence that the firm could pay its debts. In February, Credit Suisse reported an unexpected write-down of $2.8 billion that CEO Brady Dougan attributed to "mismarkings and pricing errors by a small number of traders in certain positions" in the company's structured credit business. Kareem Serageldin, Credit Suisse's recently appointed global head of collateralized debt obligations, was among employees suspended after an internal review uncovered the errors.

Dougan told analysts looking for reassurance that even with the announcement, "we feel we have actually managed our risk fairly well," but that the company still needed to "continue to focus on improving its risk management practices and procedures."

BearingPoint's Reagan observes that in the case of Société Générale, "their activities deal with high volume, high velocity and quick tempo trading of stock," and it's likely business leaders "wouldn't put up with" security measures that would slow them down. For example, Société Générale employed single-factor authentication (using one method, such as passwords, to grant access to its systems) rather than stronger dual-factor authentication (requiring that individuals employ two methods of identifying themselves to gain access).

"The security team needs to explain the risk exposure and the possibility of losing billions in fraudulent trades if security is not adequately addressed," Reagan says. "But most security guys aren't well enough in tune with the business to be able to articulate a business case like that."

That disconnect can be enormously destructive, as the Société Générale incident shows. "The Société Générale case brings to the fore the fact that business risk can be directly exposed through IT," Crawford says. "Kerviel allegedly manipulated the IT controls on the business systems based on his midoffice experience and back-office [IT] knowledge and expertise."

Between Jan. 18 and Jan. 20, the bank discovered that Kerviel had established trading positions—bets that the price of securities and warrants would move in a particular direction—that were worth more than the bank itself. He bet wrongly, and unwinding those positions over the following three days cost the bank about $7.2 billion as it sold the stocks into a falling market.

As an arbitrage trader, Kerviel should have been making transactions in pairs, buying and selling similar assets to exploit the minute and fleeting differences in prices that exist in markets. Arbitrage trading is considered less glamorous than the one-way bets he secretly made from time to time by faking one half of a pair of transactions.

A preliminary internal investigation by Société Générale noted that Kerviel had previously worked in the bank's IT department, and so had in-depth knowledge of its systems and procedures. Staff mostly followed those procedures, the investigating committee found, but the procedures were not in themselves sufficient to identify the fraud before Jan. 18, partly because of the effort Kerviel made to avoid detection, and partly because staff did not systematically conduct in-depth investigations when warning flags were raised.

Among the tricks Kerviel used to hide his activities, the bank's investigation highlighted the use of fake e-mail messages to justify missing trades, and the borrowing of colleagues' log-in credentials to conduct trades in their name. Investigators identified at least seven occasions on which Kerviel faked messages between April 2007 and Jan. 18, four of them referencing trades that never existed. The deception was uncovered when they could find no trace of Kerviel receiving the purported messages in the bank's e-mail archival system, Zantaz.

Between July 2006 and September 2007, internal control systems raised 24 alerts when the value of Kerviel's trades exceeded authorized limits, the General Inspection department reported. At the time, the bank's risk monitoring unit put the anomalies down to recurrent problems with the way the trading software recorded operations, and asked Kerviel's superiors to make sure he didn't exceed limits again.

The special committee made a number of recommendations, including the use of stronger, biometric authentication systems to prevent traders from accessing one another's accounts, and the improvement of alert procedures so warnings reach the appropriate managers. In addition, it suggests the tightening of trading controls, which do not cover cancelled or modified transactions—two of the tricks Kerviel used to conceal his bets.

Auditors are still looking for suspect trades to make sure all have been uncovered, and investigators have yet to review Kerviel's use of an instant-messaging service for evidence of his activities, the special committee said. It will present a final report to shareholders at the annual general meeting on May 27.

Meanwhile, on April 1, at a conference sponsored by Morgan Stanley, Oudea said the bank had tightened its IT security and access to its information systems, among other measures to improve its operational controls. Lessons for I.T.

Perhaps some good may come out of Kerviel's apparent fraud and Société Générale's blindness to it: The incident may spur other companies' executives to talk about risk management and IT controls inside their businesses. Organizations tend to think of access as being binary in nature: You get access to it all, or you don't, says Ian Walden, professor of information and communications law at Queen Mary, University of London. In reality, there are many more levels of access. "In modern, complicated systems, the granularity has to be much more sophisticated."

To make the best use of systems with advanced access controls, the IT department must have a thorough understanding of how the business works and where there is risk. But IT departments and business managers have yet to find a way to wrap security into business processes so it is not an impediment, Walden says.

In the Ponemon Institute study, only 30 percent of respondents said their organizations make sure user access policies are validated and checked. Meanwhile, accountability for governing access to systems is diffuse. Twenty-nine percent of respondents said business units were most responsible, followed by application owners, corporate IT, human resources, information security and compliance organizations.

EMA's Crawford says companies can begin to get a better handle on access risks by asking some basic questions. These include:

* What kind of behavior anomalies would indicate you may have more risk exposure than you realized, and can you detect or recognize them?
* Do high-level or high-risk employees have privileges that are so broad that checks and balances among individuals' duties become negated? How effective are the controls assuring that such segregation of duties could be enforced?
* Are your control systems or risk indicators subject to subversion? Are there ways you can enforce more effective controls and still be able to capitalize on new business opportunities?

"Businesses are just now beginning to awaken to the controls within the IT environment," Crawford says. "If you're betting the farm and strategy on the IT controls, it behooves the organization to ensure that those controls are reasonably resistant to subversion."

*Peter Sayer is Paris bureau chief with IDG News Service. CSO Staff Writer Katherine Walsh and IDG News Service London Correspondent Jeremy Kirk contributed to this story.*