

An Analysis of Information Security Governance Structures: the Case of Société Générale Bank

Ifeoma Udeh and Gurpreet Dhillon
*School of Business,
Virginia Commonwealth University, Richmond, VA*

Abstract—Organizations constantly experience lapses in internal organizational controls thereby affecting the information security of the enterprise. While the problem has been widely acknowledged and sufficient advances made in addressing the issues, yet incidents of gross neglect and failure of information security governance continue to increase. In this paper we analyze the latest casualty of failed security governance, the case of the French Société Générale Bank. Our analysis suggests that a skewed technical orientation in instituting controls was to blame. We propose that a more balanced approach to designing controls needs to be adopted. Such an approach would consider a range of issues at the informal, formal and technical levels.

I. INTRODUCTION

Information system security is an ongoing concern to businesses, regulators and users alike. The concern about information system security heightens with the advance in technology, and this is so not only because of increased reliance of individuals and businesses on information and communication technologies, but also because the attempts to manage information security have been skewed towards implementing increasingly complex technological controls [3]. Information systems security involves a formal, informal and technical dimensions [2], and a system is vulnerable to attack to the extent that either one of these dimensions is porous. Prior literatures have emphasized the importance of viewing information systems security from a socio-technical perspective. This stance does not underestimate the importance or role of technology, but in addition, it acknowledges the effect of the human factor. According to Dhillon [3], the violation of safeguards by trusted personnel of an organization is emerging as a primary reason for information security concerns.

Organizations of all kinds, government parastatals, public and private companies, and even nonprofit organizations, have each experienced some form of information security system breach. With the capitalistic nature of the environment in which these organizations operate, most of the information systems security breaches that make the popular media are those that have huge financial implications, in other words, those that are closely related to a fraud scheme. Such information system security breaches resulting from violation of safeguards is defined as a deliberate misappropriation by which individuals intend to gain dishonest advantages through the use of computer

systems [4]. Not to discredit the goodness in people in general, but as Brewer [1] states fraud often simply starts as good people coming together to create business solutions to satisfy some demand set by external forces. However, as the external (and maybe internal) pressure increases, so too does the ‘engineering’ of the solutions, which if not checked against some established standards, may escalate out of proportion.

Information system security breaches in general and fraud-related breaches in particular, occur as a result of three main factors: opportunity, rationalization/attitude and pressure. These factors need not all be present for a fraud-related breach to occur, as the presence of either rationalization/attitude or pressure and opportunity is sufficient to motivate and affect a fraud scheme. Opportunity may be manifested in diverse ways, and the most common is the lack of effective system controls. In addition to technical aspects such as passwords and keys, system controls involve promoting the values that a business feels are positive, and monitoring employee behaviors [3]. Rationalization or attitude focuses on the normative beliefs and the personal factors of individuals. Some people may justify an inappropriate behavior on many grounds including, that everyone is doing, or that it is the only way to survive, or that it is their right considering the compensation they receive for their hard work. The third factor, pressure, relates to expectations from both internal (e.g. management) and external (e.g. shareholders, financial analysts, market etc.) forces that demand positive and maybe extraordinary outcomes such as continuous rise the stock price.

This paper is an analysis of the recent Société Générale Bank fraud. This paper analyzes the fraud case from a control perspective, and argues that employees are motivated to indulge in fraudulent practices when adequate controls are not in place or when the established controls are not being strictly implemented. The paper is organized as follows. Section II provides some background information about the Société Générale Bank fraud. Section III presents the control structures. Section IV presents the discussion and evaluation of controls, and Section V presents the conclusion.

II. THE SOCIÉTÉ GÉNÉRALE BANK CASE

In January 2008, Société Générale Bank (hereafter SGB) disclosed that it had suffered losses, equal to more than 7 billion U.S. dollar (Euro 4.9 billion), when it unwound 50 billion Euros worth of unauthorized bets that Jerome Kerviel, an employee of the bank, hid through a series of fictitious transactions. The \$7 billion fraud is the biggest in the history of France. Jerome Kerviel, a 31 years old trader at SGB, is accused of breach of trust, fabricating documents and illegally accessing computers. SGB claim that Kerviel took unauthorized positions totaling Euro 50 billion on three European futures markets, which led to more than \$ 7 billion (Euros 4.9bn) loss. As a result of the fraud that was detected at SGB, the shares of bank were suspended from trading after falling 4.1 percent to \$115 (about 79.08 Euros). Though no evidence has been found to confirm that Kerviel had benefited personally from the fraudulent activities, he may have done so by artificially boosting his paper transactions and thus, the bonus he could claim for 2007. Kerviel was paid Euros 60,000 bonus in 2006, and in 2007, he demanded Euros 600,000, but was only paid Euros 300,000.

III. THE OPPORTUNITY

Since the late 1800s, SGB has grown to become one of the three leading French banks, and their core businesses include Corporate & Investment Banking, Retail Banking, Specialized Financial Services, Asset Management, Private Banking, Securities Services, payment Services and Suppliers. Being established and listed in a country with a communitarian view of corporate governance structures, SGB has an Audit Committee, a Compensation Committee and a Nomination Committee, and claims to implement the recommendations given in the Association Française des Entreprises Privées (Association of French Private-Sector Companies) and Mouvement des Entreprises de France (French Business Confederation) - AFEP-MEDEF, report of September 2002 on the corporate governance of listed companies. SGB has a culture that motivates their employees to achieve their goals; and the bank claims that their success over the years has been a factor of team spirit, professionalism and innovation.

With respect to trading transactions at SGB, there are controls relating to trading limit authorizations, however, Jerome Kerviel was able to circumvent these controls and post fictitious transactions totaling more than \$7 billion. Jerome Kerviel was the sole architect of an elaborate fraud involving scores of fake transactions. Jerome's exposure to the banking industry and the manner in which trades are conducted made him aware of the internal controls and the lapses that existed in the internal controls at SGB. More so, Jerome has a brother Olivier Kerviel, who until recently was a former trader at BNP Paribas (the leading French Bank), but Olivier left BNP Paribas after acknowledging to an unrelated trade that caused losses to a client. As such,

Jerome Kerviel had knowledge about the shortcomings that may exist in internal controls, and manipulated the system.

The management was passive and negligent about the details of the trades that were conducted by Kerviel that they later blamed for losses of more than \$7 billion (4.9 billion euros). Management failed to follow up and investigate further unacceptable trade practices that they witnessed. Kerviel made speculative bets on the order of 500 million (\$770 million) to 600 million euros (\$925 million), at the workstation of his direct superior, Eric Cordelle, and in his presence, when the maximum authorized ceiling for the desk was Euro 125million. Kerviel unwound the fake transaction positions that he posted from his superior's computer within a day or transferred them to his own computer, from where he either erased them immediately or kept them. When he maintained the fake positions for longer than a day, it was without Cordelle's knowledge. However, though Eric Cordelle initially denied knowledge of the fake transactions, and stated that the necessary software to post transactions was not even installed on his computer, he subsequently admitted that he had witnessed Kerviel taking intraday positions and making unauthorized trades on the computer of a junior trader Bu-Ly Wu, for a few hours as part of his training and confronted him.

Further, the management of SGB ignored the several warnings in 2006 that should have led them to investigate Kerviel's activities more closely. The findings released by a panel of independent SGB board members indicate the bank supervisors and the bank's compliance officers had failed to follow up on at least 75 internal alerts raised by Kerviel's activities. In particular, the findings indicate that his immediate superior was made aware on several occasions of the irregular trades but failed to take action. These findings suggest that Kerviel's actions were tolerated while he was on a winning streak. Similarly, the 27-page interim report commissioned by the three-man crisis committee, paints a picture of lax supervision in which controls appear to have been exercised in a box-ticking manner rather than through persistent inquiry. In particular, one reason the alleged fraud was not discovered in spite of concerns raised by Eurex, Europe's leading derivatives exchange, was that Kerviel's supervisor "was satisfied by the trader's explanation without verifying it". Kerviel's supervisor accepted his explanation in spite of the fact that the explanation contradicted Eurex's concerns.

On the one hand, the bank appears not to have a hotline or whistle-blower program in place, that will enable subordinates and employees in general report illicit activities that they are aware of. Kerviel claims that his assistant Thomas Mougard was aware of the fake transactions, since he had asked him to input fictitious transactions; and that Mougard carried out his instructions knowing that they concerned hiding open positions and earnings. Mougard admitted to inputting fictitious orders on

behalf of Kerviel, but stated that Kerviel had informed him that the trades were meant to cover out-of hours transactions, and that Kerviel never mentioned the multi-billion euro stakes on the stock markets. Mougard conceded that he could have entered, some trades using Kerviel's computer, and that there was the possibility that on some occasions he may have forgotten to log off when he was using Kerviel's workstation to access certain timely information. However, Mougard denied ever knowingly conducting fictitious transactions.

More so, the committee's report stated that there were also no controls on cancelled or modified trades. These were techniques allegedly employed by Kerviel in effecting and unwinding the fake trades. The report also stated that the people charged with oversight over the controls did not routinely inform superiors about anomalies even those involving significant sums of money. Though, no evidence of collusion or of self-enrichment on Kerviel's part was found, the 400% increase in his bonus was a significant change that could have been traced to the sharp change in his trading record, and that could arguably have raised suspicions. Further, although no evidence of accomplices was found, the possibility of the existence is not ruled out, especially in view of the extended internal network of personal relationships that Kerviel had, in particular with the support and control teams.

IV. PREVALENT NORMS

Like many other merchant banks, SGB rewarded their employees with bonuses, which are based on the level of profitability contributed by the employee. The bonus offered were substantial considering that SGB is one of the three leading banks in France. Hence, employees are motivated to be innovative and increase their contribution towards the company profits. More so, SGB over the years has proven to be performance-oriented, such that even in its early days, during the dark years, 1871 to 1893, when France went through a period of economic gloom marked by the failure of several banking establishments, SGB continued to grow at a moderate but steady pace. This demonstrates the bank's capacity to withstand unfavorable economic conditions. Such a drive to succeed at the corporate level has filtered down to the employees and has become a culture in the organization.

Nonetheless, there seems to be an underlying culture to shirk responsibilities even when comparable authorization exists. This evasion of responsibilities results in a lack of accountability. With the fraud at SGB and the reported lack of control, many criticisms have been made against the system and those charged with governance. The French President, Nicolas Sarkozy stated that he was baffled by bank's board loyalty to the CEO. After the discovery of the fake transactions, in late January 2007, Daniel Bouton offered his resignation but the bank's board rejected the offers partly out of fear that a change at the helm then might

derail a 5.5 billion euro emergency share sale aimed at shoring up reserves that had been depleted as a result of the scandal. The French President stated that it is not normal for a president of a company to experience a disaster of this magnitude and not face any consequences. Neither the CEO nor any member of management accepted responsibility whether directly or indirectly for the fraud. The CEO Daniel Bouton implicitly assumes responsibility for the success of the bank by demanding to be paid seven million euros a year, however, the CEO failed to assume a similar responsibility when there was a problem.

Further, as commented by Walt Lukken, the top U.S. futures markets regulator, industry participants can become complacent about their own practices, even when they may be following all of their regulator's rules. SGB though it had implemented the corporate governance requirements, was unworried about the daily practices of the employees. Such practices as using others computers to post trades and authorizing trades that were above a trading desk's limit are just a few of the practices that should have signaled to management that controls needed to be evaluated. Also, the fact that such practices were what resulted in the \$7 billion fraud, according to Lukken, merely reinforces the basic view that smart business practice extends beyond "checklist regulation. Further, such practices, and the fact that they are allowed to go unchecked in the bank raises concerns about the tone of ethics prevalent in the bank.

V. EXTERNAL VARIABLES

In France, corporations are seen as social organizations having a legal status accorded by the Society, and are expected to act in the best interest of the society, meeting social responsibilities, and not just the demands of the shareholders. France has detailed regulations specifying the social responsibilities of firms towards the communities and most large publicly traded firms are state-controlled. Though SGB is a publicly traded firm that responds to the demands of the investors, being a major organization in France, the government takes interest in the bank, and is concerned about its success. With the discovery of the over \$7 billion fraud and the subsequent decline in the shares of SGB, the bank may have seemed a good "prey" for a merger, but the French President Sarkozy is determined to keep SGB as a French institution for both economic and political reasons, in view of the speculations about potential mergers with other non-French institutions, such as Unicredit and Intesa Sanpaolo, of Italy, and Banco Santander, of Spain; and the fact that a merger between a French bank such as BNP Paribas and SGB, each with a sizable investment banking businesses, would probably result in significant layoffs.

To remain viable and meet the demands of the shareholders, in view of the fraud discovery, SGB had a 5.5 billion euro share sale. This right issue was aimed at helping SGB recover from approximately Euros 4.9 billion

of losses due to the unauthorized trading activities of Jerome Kerviel, and a further Euros 2.6 billion write-down on sub-prime exposure in the American mortgage securities market. SGB initiated and completed the rights issue of 5.5 billion euros to bolster its capital. The share sale was a success, attracting demand from investors for nearly twice the number of shares offered. Though the rights issue was heavily oversubscribed, much of the success is due to the sub-prime crisis, which has forced potential predators to withdraw their advances. Banks such as BNP Paribas pulled out of a merger deal with SGB because of the financial turbulence, unpredictable share movements and the fear of hidden losses that are high possibilities with respect to SGB current situation. Also, Credit Agricole, the French bank that had officially signaled interest in SGB did not pursue further the merger.

Pressures from across the globe continue to worsen the situation at SGB. The sub-prime mortgage market crisis is ongoing and recently, Cohen Milstein Hausfeld & Toll, a New York law firm that specializes in class action cases, filed a lawsuit against SGB in a federal court in New York, alleging that the bank misled American investors by failing to inform them about its sub-prime mortgage market exposure, Kerviel's unauthorized dealings, and for failing to act on information provided to them about Kerviel's trades.

VI. CONTROL STRUCTURES

Quite a lot has been documented in prior literature about internal control especially since the recent accounting scandals involving Enron, WorldCom, and Tyco, and the enactment of Sarbanes-Oxley Act of 2002. The latter resulted in landmark changes in the field of accounting in general and in public accounting, in particular. Internal control, in the accounting community, is typically defined rather narrowly as a tool to promote reliable financial reporting, and in view of that public companies that are subject to the U.S. Sarbanes Oxley Act of 2002 are encouraged to adopt the Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Internal Control - Integrated Framework" or the Control Objectives for Information and related Technology (COBIT).

COSO Internal Control - Integrated Framework states that internal control is a process, established by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of stated objectives. COSO control objectives focuses on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for IT management created in 1992. COBIT approaches IT control by focusing on information (not just

financial information) that is needed to support business requirements and the associated IT resources and processes. As such, COBIT is useful for IT management, users, and auditors.

TABLE 1
COMPARISON OF COBIT (PLAN & ORGANIZE DIMENSION), COSO, AND IT DIMENSIONS

COBIT	COSO	IT Dimensions
Define a Strategic IT Plan and direction	Control environment	Formal
Define the Information Architecture	Control environment	Technical
Determine Technological Direction	Risk Assessment	Technical
Define the IT Processes, Organization and Relationships	Control Activities	Formal
Manage the IT Investment	Control Activities	Formal
Communicate Management Aims and Direction	Information and Communication	Formal and Informal
Manage IT Human Resources	Control Activities	Formal and Informal
Manage Quality	Control Activities	Formal and Informal
Assess and Manage IT Risks	Risk Assessment and Monitoring	Formal, Informal, and Technical
Manage Projects	Control Activities and Monitoring	Formal, Informal, and Technical

Though a one-to-one mapping of the five COSO control components and the four COBIT objective domains may not be possible as each framework is targeted at a different audience, the intent of this paper is to evaluate the similarities between the COSO framework and the first of the four domains of the COBIT framework, with respect to the dimensions of Information Technology (Formal, Informal and Technical), and on that basis, discuss the internal and/or external control issues at SGB.

The COBIT framework consists of four domains: plan and organize, acquire and implement, deliver and support, monitor and evaluate. However, as mentioned above, the focus of this paper is on the plan and organize dimension. The Planning and Organization domain involves the use of information & technology, and the organizational and infrastructural form IT should take in order to achieve the optimal results. It includes ten high level control objectives (Table 1). The COSO Internal Control - Integrated Framework consists of five interrelated components: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Risk assessment is an entity's identification and analysis of relevant risks to the achievement of its objectives. It forms a basis for determining how the risks should be managed. The

control activities are the policies and procedures that help ensure that management directives are carried out. The activities help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Information entails the identification, capturing, distribution and use at all levels of the entity, relevant, reliable and timely information in a form that supports the achievement of the objective. Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control. Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions.

VII. DISCUSSION AND EVALUATION OF CONTROLS

The discussion on the SGB's alleged fraud case and the actions of Kerviel indicate an intentional breach of the information security system via the violation of safeguards. Dhillon [3] defined information system security breaches resulting from violation of safeguards as a deliberate misappropriation by which individuals intend to gain dishonest advantages through the use of the computer systems. Though from case it appears that Kerviel did not benefit directly from his fraudulent activities, but his subsequent demand for an enormous bonus may have been part of the whole scheme intended to benefit him in a manner that seemed legal.

Though it appears that SGB has designed and implemented an internal control system, which to a great extent addresses the technical dimensions, the flaw relates to the operating effectiveness of the established system. The formal and informal dimensions, but primarily the formal dimension was extensively porous.

A. *Formal Dimensions*

The need for organizations to design, implement, and monitor the operating effectiveness of its policies as it relates to information systems security can not be overemphasized. Formal security policies and procedures will facilitate communication and minimize ambiguity and misunderstandings with an organization. Management is responsible for the process of establishing these formal policies. It is in their responsibility to influence employees towards the good, and provide an environment for them to achieve organizational objectives. By setting the tone for the organization, management establishes a basic pattern of shared assumptions, values, and beliefs considered to be the correct way of thinking about and acting on problems and opportunities facing the organization [5].

It is as important to enforce these formal policies as it is to establish them. Pressures from within and/or from outside the Organization, including but not limited to those relating to profitability, may make employees overlook

established policies, or make management relax the enforcement of the policies. The SGB case suggests that for reasons relating to the improved financial performance resulting from the fictitious trades, management failed to adhere to the multiple "red flags" that may have led to an earlier discovery of the alleged fraudulent practices of the trader Kerviel. Also, as the responsibility structure is an integrated part of the formal dimension, it becomes relevant to question if the multiple sources of the "red flags" could have pursued further their suspicion, after all they were unaware if the management level to which they reported to, was a part of the whole scheme. Further with respect to the authorized trading limits and using others computers, Kerviel's superior could have done much more than comment. At the least, he could have been suspended for some days which would have disrupted his fraudulent trading.

Similarly, the SGB case suggests that overall, the top-down and down-up communications at the bank is at best, skeletal. Information is not communicated timely and appropriately to the targeted recipients. And even when communicated, it appears the recipients do not act on the information received accordingly. From the case, the perceived culture, which seems to be the dominant culture, is one of lackadaisical attitude towards information systems security risk. The underlying reason for such an attitude may stem from an optimistic bias and illusion of control as it relates to information systems security [6].

More so, Kerviel's fraudulent activities spanned for about a year, and within this year internal control procedures were evaluated by two global auditing firms – Ernst & Young and Deloitte & Associates, and both in their combined report had no matters to report. This has implications for the quality of work performed by auditors both internal and external auditors. However, the discussion relating to the effectiveness of auditors is beyond the scope of this paper.

B. *Technical Dimensions*

SGB appears to have an established policy about authorized trading limits, however, these policies failed to be implemented. From a technical perspective, one would think that each trading desk would not be allowed by the system to post transactions above the set limit. This may be possible via matching the access code/password to the limit authorized and then granting or denying passage. However, since Kerviel was able to post fake transactions above the authorized limit, it indicates that there is a lack of agreement between the formal and the technical dimensions. Needless to mention, but all the three dimensions of information security systems ought to function in unison. More so, the fact that Kerviel was able to use others computers for trading purposes, indicate that either this risk has not been assessed by the organization, or

it has been assessed, but that management did not consider it important enough as to address it.

C. *Informal Dimensions*

From the SGB case, not much was observed with respect the informal dimension. However, it is important to point out that the employees functioning in any capacity within an organization should not allow their personal relations with their colleagues to cloud their judgment, impair their objectiveness or professional skepticism. Whether or not it was the alleged culprit's intent from the onset, his relationship with those in the support and control team may have affected their decisions even when they observed the abnormalities with respect to his activities.

VIII. CONCLUSION

This paper has presented an analysis of the breach of information systems security through a discussion of the recent fraud perpetrated by a security trader at the Société Générale Bank. The paper suggests that the implementation and operating effectiveness of controls particularly the formal controls is as important as the design and implementation of such controls, and that it is the responsibility of management to enforce both. Thus it is important that within an organization that management establishes and implements effective policies and procedures relating to internal controls and that these are communicated to employees via formal, informal and technical approaches. More so, monitoring should be a core part of the information security system. This suggests that abnormal activities should be fully investigated and not just waved by, and culprits should be appropriately reprimanded. Thus, to prevent adverse occurrences, management ought to set the tone from the top and maintain the tone set.

REFERENCES

- [1] L. Brewer., "Is there a little bit of Enron in all of us?," *The Journal for Quality and Participation*, vol. 30(1), pp.26-28, 2007.
- [2] G. Dhillon, *Principles of Information Systems Security*. New Jersey: John Wiley & Sons, Inc., 2006.
- [3] G. Dhillon, Gurpreet. "Violation of safeguards by trusted personnel and understanding related information security concerns," *Computers & Security*, vol. 20(2), pp. 165-172, 2001.
- [4] G. Dhillon, and S. Moores, "Computer crimes: theorizing about the enemy within," *Computers & Security*, vol. 20(8), pp. 715-23, 2001.
- [5] S.L. McShane, and M.A. Von Glinow, eds. *Organizational Behavior*, 2nd ed., New York, NY: McGraw Hills, 2003.
- [6] H.S. Rhee, Y.U. Ryu, and C.T Kim, "I am Fine but You are Not: Optimistic Bias and Illusion of Control on Information Security," *International Conference on Information Systems*, Las Vegas, NV, 2005.