a rogue trader at societe generale roils the world financial system

Law, Security

1. What concepts in this chapter are illustrated in this case? System vulnerabilities

Computer crime: using computers as instruments of crime to defraud the bank, customers, and other financial institutions Internal threats from employees: Jerome Kerviel has access to privileged information; he was able to run through the organizations system without leaving a trace Business value of security and control: Organizations can be held liable for needless risk and harm created if the organization fails to take appropriate protective action to prevent loss of confidential information, data, corruption, or breach of privacy.

Information system controls: General controls: govern the design, security, and use of computer programs and the security of data files in general throughout the organizational information technology infrastructure Application controls: automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application.

Risk assessment: determines the level of risk to the firm if a specific activity or process is not properly controlled Security policy: drives policies determining acceptable use of the firms information resources and which members of the company have access to its information assets The role of auditing: an MIS audit examines the firms overall security environment as well as controls governing individual information systems

2. Describe the control weaknesses at SocGen. What management, organization, and technology factors contributed to those weaknesses?

One former SocGen risk auditor, Maxime Legrand, called the control procedures used to monitor the activity of its traders a sham and that the management pretend(s) to have an inspection to please the banking commission.

Management: Jerome Kerviel's supervisors saw a balanced book when in fact he was exposing the bank to substantial risk because of the way he entered the transactions. Kerviel worked late into the night long after other traders had gone home and took only four vacation days over the course of 2007 to prevent his activities from being detected. Managers did not enforce vacation policies that would have allowed them to scrutinize his work while he was gone. Supposedly he used his managerial computer to execute several of his fraudulent trades while the manager watched him. Kerviel's defense lawyers argue that he acted with the tacit approval of his superiors during his more successful initial period of fraudulent activity.

Organization: Jerome Kerviel gained familiarity with many of the company's security procedures and back-office systems. He was then moved to another job in the company in which he could use that knowledge. He knew the schedule of SocGenas internal controls which allowed him to eliminate his fake trades from the system just minutes prior to the scheduled checks and re-enter them soon after. The temporary imbalance did not trigger an alert. The bank ignored many warning signs that Kerviel was capable of the level of fraud that he committed. The bank failed to follow up on 75 warnings on Kerviels positions over the course of several years.

Technology: Jerome Kerviel was able to use other employee’s access codes and user information to enter fake trades. The system failed to detect that Kerviel performed legitimate transaction in one direction, but falsified the hedges that were supposed to offset the legitimate ones. He entered false transactions in a separate portfolio, distinct from the one containing his real trades. No system detection software was installed to detect these transactions. SocGens controls were capable of detecting more complicated errors and fraudulent transaction than the simple ones that Kerviel allegedly committed.

3. Who should be held responsible for Kerviels trading losses? What role did SocGens systems play? What role did management play?

Managers and executives at SocGen should be held responsible for Kerviel’s trading losses. They are the ones who should be setting policies and enforcing them to prevent these kinds of activities from taking place.

SocGens systems were capable of detecting complicated errors and fraudulent transactions that were more sophisticated than those committed by Jerome Kerviel. Yet he was able to commit very simple fraudulent transactions that went undetected. System controls obviously were not as thorough or as strong as they should have been. There were several other system vulnerabilities that Kerviel was able to exploit to commit his crime.

Managers aided Jerome Kerviels activities by deciding to unload his positions soon after discovering the fraud, despite the fact that the market conditions at the time were decidedly unfavorable. That led to even greater problems in the global financial world. The SEC launched an investigation into whether or

not SocGen violated U. S. securities laws by unwinding Kerviels positions covertly after the fraud was revealed as well as whether or not insider information played a role in the selling of SocGen stock prior to the announcement of the scandal.

4. What are some ways SocGen could have prevented Kerviel’s fraud?

Instituting access controls to prevent improper access to systems by unauthorized insiders and outsiders. The bank could have used authentication technologies like tokens, smart cards, or biometric authorization instead of simple passwords. That would have prevented Kerviel from being able to use other employee’s access codes to enter transactions.

Intrusion detection systems could have been installed that would have detected much of Kerviels activities. These systems generate alarms if they find a suspicious or anomalous event. They also check to see if important files have been modified. Monitoring software examines events as they are happening to discover security attacks in progress. Many of Kerviels false offsetting transactions could have been detected using one of these systems. Stronger auditing procedures should have been in place and enforced. Auditors can trace the flow of sample transactions through the system and perform tests, using automated audit software.

Using computer forensic techniques and technologies would have helped. Electronic evidence resides on computer storage media in the form of computer files and as ambient data which are not visible to the average user. Data that Kerviel deleted on the bank’s storage media could have been

recovered through various techniques. The data could have been used as evidence at his trial and in follow-up investigations.

5. If you were responsible for redesigning SocGens systems, what would you do to address their control problems?

General controls: govern the design, security, and use of computer programs and the security of data files in general throughout the organizations information technology infrastructure. These controls address software controls, physical hardware controls, computer operations controls, data security controls, controls over implements of system processes, and administrative controls.

Application controls: specific controls unique to each computerized application. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by applications. Application controls include input controls, processing controls, and output controls.

Acceptable use policy: SocGen should create an AUP to define acceptable uses of the firms information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.