cover her tracks. Stephanie was able to embezzle, on average, $125,000 a month. About 16 months after she began working at Cleaver, the controller saw her at a very expensive French restaurant one evening, driving a Jaguar. He told the internal auditors to keep a close watch on her, and they were able to catch her in the act.

Required

a. What weaknesses in the organization's control structure must have existed to permit this type of embezzlement?

b. What specific control techniques and procedures could have helped prevent or detect this fraud?

5. INPUT CONTROLS AND NETWORKING

A global manufacturing company has over 100 subsidiaries worldwide reporting to it each month. The reporting units prepare the basic financial statements and other key financial data on prescribed forms, which are e-mailed or faxed to the corporate headquarters. The financial data are then entered into the corporate database from which consolidated statements are prepared for internal planning and decision making.

Current reporting policy requires that the subsidiaries provide the previous month's reports by the tenth working day of each new month. Accounting department staff log and enter the reports into the database. Approximately 15 percent of the reporting units are delinquent in submitting their reports and three to four days are required to enter all the data into the database. After the data are loaded into the system, data verification programs are run to check footings, cross-statement consistency, and dollar range limits. Any errors in the data are traced and corrected, and reporting units are notified of all errors via e-mail.

The company has decided to upgrade its computer communications network with a new system that will support more timely receipt of data at corporate headquarters. The IT department at corporate headquarters is responsible for the overall design and implementation of the new system. It will use current computer communications technology and install LANs, PCs, and servers at all reporting units.

The new system will allow clerks at the remote sites to send financial data to the corporate office via the Internet. The required form templates will be downloaded to the remote sites, along with the data verification programs. The clerks will enter data into the forms to create a temporary file, which data verification programs will check for errors. All corrections can thus be made before transmitting the data to headquarters. Either the data would be transmitted to corporate headquarters immediately, or the corporate headquarters computer would retrieve it from disk storage at the remote site as needed. Data used at corporate headquarters would therefore be free from errors and ready for consolidation.

The company's controller is pleased with the prospects of the new system, which should shorten the reporting period by three days. He is, however, concerned about security and data integrity during the transmission. He has scheduled a meeting with key personnel from the systems department to discuss these concerns.

Required

The company could experience data security and integrity problems when transmitting data between the reporting units and corporate headquarters.

a. Identify and explain the data security and integrity problems that could occur.

b. For each problem identified, describe a control procedure that could be employed to minimize or eliminate the problem. Use the following format to present your answer.

Problem Identification and Explanation	Control Procedure and Explanation

6. PREVENTIVE CONTROLS

Listed here are five scenarios. For each scenario, discuss the possible damages that can occur. Suggest a preventive control.

a. An intruder taps into a telecommunications device and retrieves the identifying codes and personal identification numbers for ATM cardholders. (The user subsequently codes this information onto a magnetic coding device and places this strip on a piece of cardboard.)

b. Because of occasional noise on a transmission line, electronic messages received are extremely garbled.

c. Because of occasional noise on a transmission line, data being transferred are lost or garbled.

d. An intruder is temporarily delaying important strategic messages over the telecommunications lines.

e. An intruder is altering electronic messages before the user receives them.

7. OPERATING SYSTEM RISKS AND CONTROLS

Listed here are four scenarios. For each scenario, discuss the potential consequences and give a prevention technique.