Bank Fraud Newsletter

Investigator's Corner

by David E. Zulawski and Douglas E. Wicklander

"Back to the Basics"

Olympic athletes practice their skills to become the best in the world. When their skills begin to falter, their coaches often return to the basics to reinforce the foundation. In banking, the basics sometimes are forgotten in the haste to move ahead.

Simple things constitute the foundation of the loss prevention function of banking. Audits, double checking work, and other seemingly simple tasks may seem inconvenient and after a while unnecessary. When a control is eliminated, however, an opportunity is created for a dishonest person to take advantage of the weakness.

Cash Accountability

Fundamental to the bank's security is accountability for cash in the vault and on the teller line. Many investigations are made unnecessarily complicated by a lack of controls on the facility's cash. How is the access to your vault controlled?

What begins as a firm rule about who may enter the vault and under what circumstances weakens as employees get to know one another. When trust comes at the expense of security awareness, it must be tempered. Trust is ensured and enhanced by attention to the rules and regulations of cash handling. Employees are most comfortable with rules that define their practices. Consistency in the way cash is handled and transferred also limits the bank's exposure to loss.

Consider the following areas of potential exposure and whether your bank is a protected adequately:

1. How is cash transferred from the vault to the teller?

2. How is the teller's cash controlled and protected?

3. Does the teller have the ability to lock his or her drawer when off the teller line?

4. Is the teller's cash adequately controlled when the teller is not working?

5. Are surprise cash audits conducted regularly on the vault and teller funds?

6. Is the physical security of the funds adequate? Are drawers and locks in working order.

7. Do supervisors monitor the teller's drawer security? Are tellers warned about leaving their drawers unsecured even momentarily?

8. Are tellers leaving on vacation audited?

9. Are tellers tested with overages to monitor their honesty?

10. Are tellers who resign allowed to continue working with the cash?

11. Are cash variances treated as a serious problem that is explored fully?

12. Does the bank have a policy regarding teller shortages?

13. Does the supervisor document problem tellers and initiate progressive discipline?

14. Are tellers ever allowed to work out of another's drawer?

15. Are records of the surprise audits kept on file and reviewed by senior management?

16. Are teller funds balanced at the conclusion of the work shift or do they wait until the following day ends? Physical Security

Another aspect of loss prevention is the physical security of the facility. Management changes may create confusion over who is responsible for the monitoring of the physical security of the bank, ATM and drive-up locations. Like all loss prevention functions this area should be monitored by senior management.

Consider the following questions when reviewing the physical security of the facility:

1. What are the crime statistics for the areas served by the bank?

2. Are there structural barriers to protect the vault and teller line?

3. Is access to controlled areas limited to those with a need to be in the area?

4. Is access controlled by key and/or card systems?

5. Are locks and security codes changed when employees leave or are transferred?

6. Is a master list maintained with current key and alarm code assignments?

7. Does the physical layout, neighborhood, or crime rate indicate the need for a uniformed security officer?

8. Is the alarm system tested regularly?

9. Are the security Attorney Programs tested and working properly?

10. Are the tellers trained on how to react and what to observe during a robbery or fraud?

11. Are there robbery packages in each teller drawer? Are they periodically inspected?

12. Does senior management conduct regular security inspections of the facility?

13. Is the parking area well lit?

14. Is the ATM well lit and the camera working? Proprietary Data

The physical protection of the bank's cash, customers, and employees is only one aspect of the physical security. The use of computers to automate systems has created the necessity to protect bank and customer data. This area must be protected from threats from without as well as within. It should be restricted to associates with a need to enter and it should be controlled by key or card access systems.

Some areas to consider in evaluating risk in the computer area are:

1. Is there key or card access control to restrict entrance?

2. Is entrance to the area limited to those who work there?

3. Are the data regularly backed up and safeguarded?

4. Is waste paper shredded or disposed of in a similar manner?

5. Are changes in the system monitored by management?

6. Is access to the system itself controlled by codes?

7. Are codes changed periodically or when employees leave or transfer from the facility?

8. Is there a disaster plan prepared to assure continued service in the event of a natural or manmade disaster? Investigation

The organization should have prepared for the possibility that a loss will occur. Knowing who will be responsible for the investigation and what resources are available goes a long way toward resolving such incidents successfully. As with any confidential matter the investigation should be limited to those with a need to know. A careful reaction in the early stages of the investigation often helps resolve the case.

Planning for the investigation, monitoring policies and procedures, and being aware of the facility's physical security are all part of preparing for the worst.

The questions included in this column are by no means exhaustive, but they will introduce the areas considered in a security survey. Paying attention to the basics protects your organization's assets.