The Security Officer's Role

Last updated
December 28, 2012

SECURITY EDUCATION SYSTEMS

THE SECURITY OFFICER'S ROLE
TABLE OF CONTENTS

Segment contents include . . .

These tools are also available in the "Banker Tools" section of BankersOnline (www.bankersonline.com):

- Regulation H - 12 CFR Part 298 Subpart F (FRB)
- 12 U.S.C. 1882 Part 326 -- Minimum Security Devices And Procedures And Bank Secrecy Act (FDIC)
- Part 748 of the NCUA Rules and Regulations (NCUA) & Section 5193 NCUA Accounting Manual
- NCUA Letter to Credit Unions -- LETTER NO. 02-CU-12 (NCUA)
- 12 C.F.R. Part 21 12 CFR Part 21 -- Minimum Security De-

vices and Procedures, Reports of Suspicious Activities, and Bank Secrecy Act Compliance Program (OCC)

- Compliance Laws & Regulations -- Section 405 (OTS)

Introduction

Are you your institution's Security Officer? If you are, your primary duty is to develop and administer a written Security Program for your institution. This is not an option -- it is a regulatory requirement. And even if it wasn't a requirement, initiating and maintaining an effective Security Program just makes good business sense. The Security Program should combine procedural security techniques with physical ones.

Security isn't just about alarms, robbery procedures and filing Suspicious Activity Reports. Security is the evolutionary process through which we provide a safe and secure environment for our employees to work and our customers to do business. While you don't have to be a full-time Security Officer to be professional, you do have to be a professional Security Officer -- regardless of how much time that you can devote to the role. And no one person needs to perform all of the security-related tasks within the institution. As long as there is an appointed and authorized Security Officer, he/she can delegate the performance of necessary tasks to several people -- both employees and contractors, if it's necessary -- and simply monitor the results.

Do you work for an independent, community institution? If you do, the FBI and other law enforcement agencies have warned you repeatedly that institutions such as yours are the primary targets for robbers, money laundering offenses and counterfeit check schemes. Your institution is at a greater risk to these losses than are larger institutions located in metropolitan areas.

Independent, community institutions generally operate with slim staffs made up of people who have many -- and often conflicting -- duties and responsibilities. Loss prevention, security and operational risk management practices are often overlooked or sacrificed because so many other things are considered more important. The Security Officer who works within this type of institution frequently has no more than an hour or two a week to dedicate to "working security".

Are you a full-time Security Officer? If you are, you may be following the emerging industry-standard guidelines -- one full-time Security Officer is needed for each institution that maintains a combined total of fifteen branches and departments. In other words, if you are responsible for providing security services for fifteen institution components (a combination of cash-handling facilities and departments), you have plenty of security-related tasks to keep you busy.

Many Security Officers are restricted to providing security for branch (cash-handling) operations only. But industry-standard security practices should be applied to every department, function and facility within the institution. Special attention should also be given to those activities that traditionally contribute to the greatest losses -- the institution's data processing, lending, contract and purchasing functions.

What are "industry-standard security practices?" The three (3) most common descriptions used to categorize policies, procedures and practices are:

- *Industry standard practice:* A practice or technique that is used by most of the

businesses within a specific industry;
- *Best practice:* A practice or technique that will be applied universally in the best of all worlds; and
- *Appropriate practice:* A practice or technique that works.

Industry-standard security practices aren't created or recognized overnight. Like "security", these practices evolve over time -- and generally through the "trial and error" process. Unfortunately, many of these practices remain in use long after they should have been amended or terminated. The financial services industry is full of practices that are conflicting, outdated or that need improvement. The Security Officer can play a vital role in determining which of the institution's security practices:
- Are still appropriate;
- Need updating; or
- Need to be terminated.

Each of the examining agencies has developed requirements and guidelines for developing and administering the financial institutions' security practices. The emerging industry-standard practice is that banks, thrifts and credit unions should all follow the guidelines developed for banks -- in addition to their own regulator-specific requirements.

These workbook materials rely upon the *Bank Protection Act* (an act passed by Congress) and *Regulation H* (a FRB regulation) as models. The verbatim regulations that address security requirements for all types of financial institutions may be located on BankersOnline (www.BankersOnline.com).

The Bank Protection Act and Regulation H require that the board of directors of each institution insures that:
- A Security Officer has been appointed to manage the Security Program;
- The Security Program is available in written form;
- Each facility is equipped with appropriate security devices;
- Appropriate security policies and procedures have been developed and implemented to discourage robberies, burglaries, and larcenies -- and to assist in identifying and apprehending persons who commit such acts;
- A training program is developed for and delivered to officers and employees about their responsibilities under the Security Program and in proper employee conduct during and after a robbery, burglar or larceny; and that
- The Security Officer report at least annually to the board of directors on the implementation, administration, and effectiveness of the security program.

The Problems

There are at least three (3) significant problems that the Board of Directors will likely encounter, as it develops a strategy for selecting, training and supporting the Security Officer:
1. **Selecting** the most appropriate person to fill the Security Officer position;
2. **Training** the Security Officer appropriately so that he/she can perform his/her duties in a professional manner; and
3. **Supporting** the Security Officer with the appropriate amount of time, resources and money -- not just to fulfill regulatory requirements, but to also address a

professionally-run Security Department's priorities.

The First Problem: Appointment

The first problem is to select and formally appoint the most appropriate person for the job. Unfortunately, on an industry-wide scale, more Security Officers are "appointed" to -- or "drafted" for -- the position than apply for it. And, because many Board members don't really understand what the **Bank Protection Act** or **Regulation H --12 CFR Part 298 Subpart F** requires or what the Security Officer's job involves, they don't adequately prepare or support the person that they select to fill the position.

The Bank Protection Act and Regulation H state that it is your institution's Board of Directors that is responsible for designating a Security Officer, who has the authority to research, develop and implement the institution's Security Program. The Security Officer's position often does not require full-time staffing, but the Board should carefully consider both the potential candidates' qualifications and his/her available time that may be dedicated to addressing security issues. Emerging industry-standard professional qualifications for an institution's Security Officer include:

- Holding at least a mid-to-upper-level manager's or executive's position (if you have the responsibility for achieving results but you also have no power, you'll never get anything done);
- Membership on the institution's Executive Committee (you can't protect the institution and its personnel unless you know what's going on at all organizational levels);
- The ability to report directly to the Board of Directors or an independent audit committee about security matters (you must have a guarantee of absolute confidentiality and the ability to investigate everyone's activities);
- Experience in several operational areas (you have to be able to relate and apply security principles and procedures to all functions);
- Education regarding business management, occupational health and safety, and the administration of justice fields (you will function as the manager of a business unit, a safety inspector and as a "company cop");
- Not also being the auditor (your auditor should act as your investigative companion and as the person who documents investigations); and
- The fulfillment of other duties, so long as those duties do not compromise internal controls (someone has to watch you, too).

The Second Problem: Training

The second problem is to train the new Security Officer. What does the Security Officer have to know? Not everything -- just where to find everything. You become a "resource" person and a "detective" -- finding, investigating and protecting the relationships shared with the five (5) industry-standard priorities of the Security Department, including the protection of:

- Employees, insiders and institution-affiliated parties;
- Customers, vendors and third-party service providers;
- Facilities that the institution owns, manages, maintains or controls;
- Assets that are both tangible and intangible; and
- Records and documents that exist in all forms, paper and electronic.

Neither the Bank Protection Act nor Regulation H requires that the Security Officer be trained about security practices. Regulatory agencies may develop a "field practice", however, that mandates training for a Security Officer. Providing initial and continuing training for the Security Officer will lessen both the institution's and the Security Officer's liability in many areas. In addition to state and national membership associations, other private sources are involved with developing industry-standard security practices and offering various levels of training to Security Officers, including:

- American Society for Industrial Security (www.asisonline.org);
- Association of Certified Fraud Examiners (www.cfenet.com);
- BankersOnline (www.bankersonline.com);and
- Local "peer" groups whose membership includes representatives from law enforcement and prosecuting agencies, retailers and financial institutions.

The Third Problem: Support

The third problem is to support the institution's Security Officer. Your institution's primary goals should be to provide effective customer service and to generate a profit. Often, the security function is perceived as an impediment to attaining these goals. A wise Board of Directors recognizes that a well-trained and professional Security Officer will help the institution keep more of the profits that it makes by creating a "customer-friendly" -- but "offender-hostile" -- business environment.

An institution's Board of Directors that has a clear vision of the security function is often the key to the Security Officer's success. A Board can best support the efforts of the institution's Security Officer by:

- Insisting upon a "security-conscious" organizational attitude;
- Developing and adhering to a Code of Conduct;
- Requesting a security "update" and related briefings more frequently than regulatory agencies' annual requirement;
- Requiring that all employees attend security training meetings, particularly the institution's executives and directors;
- Participating in a security training program that affects Board responsibilities;
- Carefully reviewing budget requests for new or enhanced security devices, particularly non-traditional ones; and
- Recognizing that most security matters, like many other institution-related matters, are confidential.

The Institution's Security Program

Your institution's Board of Directors should also participate in the development and annual review of the Security Program. The Bank Protection Act and Regulation H require that your directors ensure that a written Security Program for the institution's main office and branches is developed and implemented.

The literal requirements for having a Security Program may not be enough for your institution. The regulatory language, except for reporting requirements, leaves you considerable flexibility in designing the Security Program. While this flexibility allows you to design a Security Program what truly meets the special needs of your institution, it also may promote the creation of a Security Program that -- while it meets regulatory standards -- is actually ineffective or even hazardous.

To be truly effective, your Security Program must contain policies and procedures that regulate the routine activities of every function and department within your institution. The goals of these policies and procedures must be to:

- Reduce or eliminate the opportunity for mistakes, misunderstandings and crimes;
- Protect all persons on the premises;
- Identify and promote the prosecution of offenders; and
- Recover missing, stolen or lost funds.

These policies and procedures should be designed to address:

- Routine business operations;
- Unusual or suspicious events that are not crimes; and
- Your institution's potential exposure to the three types of internal and external crimes:
  - Crimes committed by document, device or technology;
  - Crimes committed by trickery or deceit; and
  - Crimes committed by force or fear.

Creating written policies and procedures for your institution should not be a complex task, although it may be a time-consuming one. If the process is complex, the resulting policies and procedures will be, also. Choose a format for creating your institution's security policies and procedures that complements the style of your existing manuals, workbooks, training guides and related documentation. Simply create an effective Security Program by making it:

- Accurate in content;
- Legal in application;
- Reasonable and appropriate for your institution's needs;
- Easy to understand;
- Simple to use; and
- An educational vehicle as well as a reference tool.

What Does The Bank Protection Act and Regulation H Really Mean?

The Bank Protection Act, the Bank Secrecy Act and Regulation H combine many long-standing policies into one process. They describe the institution's obligation to implement security procedures to discourage certain crimes, to file suspicious activity reports, and to comply with the Bank Secrecy Act's requirements for reporting and recordkeeping of currency and foreign transactions.

Security Procedures

Let's take this a step at a time. Considering the emerging industry-standard security practices, what your institution should -- and in many cases, must -- do in order to comply with regulations includes:

- **Must do**: Adopting appropriate security procedures to discourage robberies, burglaries, and larcenies, and to assist in the identification and prosecution of persons who commit such acts. These acts are described as:
  - **Robbery**: Taking something of value from a person by means of force or

fear;

- **Burglary**: Entering a building or a vehicle with the intent to commit a theft or any other crime; and
- **Larceny**: Taking something of value from a person without the use of force or fear, or misusing something that rightfully belongs to the victim -- as in embezzlement.

- **Should also do**: Develop institution-wide strategic practices for addressing all types of events, including both internal and external crimes.
- **Must do:** Having the institution's Board of Directors ensure that a written Security Program for the institution's main office and branches (cash-handling facilities) is developed and implemented. This means:
  - The Security Program must be in writing;
  - The Board of Directors must approve it;
  - The Security Program must apply to all functions located in the institution's Main Office; and
  - The Security Program should not just apply to cash-handling facilities.
- **Should also do:** Develop institution-wide, function-specific strategic practices for addressing all types of events, including both internal and external crimes.
- **Must do:** The institution's Board of Directors must designate a Security Officer, who has the authority to develop and administer a written Security Program for each banking office. This means:
  - The Security Officer should be issued a written document stating that he/she has been appointed;
  - The appointment should be reflected in the Board's minutes; and
  - The Security Officer position should have a written position description that contains appropriate duties, responsibilities and authority.
- **Should also do:** Designate qualified assistants for each critical position within the institution, and:
  - That, because this is one of the few mandatory Board-appointed positions, the Board of Directors should also designate, appoint and train an Assistant Security Officer; and
  - Provide appropriate insurance for the Security Officer and all security-related personnel.
- **Must do:** The Security Program requirements include many provisions that may affect institution-wide business operations. This means:
  - Establishing procedures for opening and closing for business (e.g., warning signals, minimum number of persons required and special circumstances);
  - Ensuring appropriate safekeeping of all currency, negotiable securities, and similar valuables at all times (e.g., safe deposit practices, vault controls and inventory procedures);
  - Establishing procedures that will assist in identifying persons committing crimes against the institution and that will preserve evidence that may aid in their identification and prosecution (e.g., standardized identification practices for customers and non-customers, detailed employment background investigations and closed circuit video cameras);
  - Retaining a record of any robbery, burglary, or larceny committed against the bank (e.g., witness statements, investigator's reports and secure evidence storage);

- ¡ Providing for initial and periodic training of officers and employees in their responsibilities under the security program and in proper employee conduct during and after a burglary, robbery, or larceny (e.g., crime-specific, position-specific and frequent training): and
- ¡ Providing for selecting, testing, operating, and maintaining appropriate security devices (e.g., using consultants, vendors and industry-standard specifications).

- l **Should also do:** Develop and implement institution-wide policy, procedure, operations and training manuals and programs for each function.
- l **Must do**: Install and/or appropriately operate the following security devices and processes:
  - ¡ A means of protecting cash and other liquid assets -- such as a vault, safe, or other secure space;
  - ¡ A lighting system capable of illuminating -- at all times -- the area around the vault, if the vault is visible from outside the banking office;
  - ¡ Tamper-resistant locks on exterior doors and exterior windows that may be opened;
  - ¡ An alarm system or other appropriate device for promptly notifying the nearest responsible law enforcement officers of an attempted or perpetrated robbery or burglary; and
  - ¡ Such other devices as the security officer determines to be appropriate, taking into consideration:
    - n The incidence of crimes against financial institutions in the area;
    - n The amount of currency and other valuables exposed to robbery, burglary, or larceny;
    - n Distance of the office from the nearest law enforcement officers;
    - n The cost of the security devices;
    - n Other security measures in effect at the banking office; and
    - n The physical characteristics of the structure of the banking office and its surroundings.
- l **Should also do:** Based upon a comprehensive risk assessment, integrate devices with processes.
- l **Must do:** Report at least annually to the institution's Board of Directors on the implementation, administration, and effectiveness of the Security Program.
- l **Should also do:** Report to the Board and the audit committee at least quarterly -- or more frequently if necessary -- on the Security Program's progress, in writing.

Suspicious Activity Reports

If the Security Officer is also the Bank Secrecy Act Officer, there are some additional requirements, including:

- l Ensuring that Suspicious Activity Reports (SARs) are filed with the appropriate Federal Law enforcement agencies and the Department of the Treasury when the institution detects a known or suspected violation of Federal law, or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act, including:
  - ¡ Known or suspected employee or other insider abuse -- regardless of the loss amount and even if there is no loss; or
  - ¡ A singular or aggregate loss of $5,000 or more in funds or other assets --

where the suspect can be identified and particularly if an alias was used; or

- ¡ A singular or aggregate loss of $25,000 or more in funds or other assets -- even if the suspect cannot be identified; or
- ¡ Transactions involving or aggregating $5,000 or more that involves money laundering, terrorist financing, identity theft or any known or suspected BSA violation; or
- ¡ Computer intrusions (excluding websites and other non-critical information systems) that are designed to compromise funds or critical information, or to disable the information system.

- l Ensuring that the institution is in compliance with all SAR instructions, including:
  - ¡ Time filing;
  - ¡ Records retention;
  - ¡ Appropriate and timely notification to the Board of Directors; and
  - ¡ Confidentiality issues.

Other Security Responsibilities

As the Security Officer, you face significant legal and operational challenges in your attempts to provide a safe and secure environment for employees to work -- and for customers to do business. Your best allies are the institution's auditor, human resources manager, compliance officer and legal counsel. With your input, the people filling these positions can provide an effective check and balance system -- to insure that appropriate prevention, identification, apprehension, prosecution and recovery strategies are developed and implemented.

Consult with your auditor, human resources manager, compliance officer and legal counsel before developing policies and procedures that may affect other departments and functions within the institution. Consult with them as you develop the institution's Security Program. They will help you to analyze the likely short-term and long-term effects of your plans. Whatever your legal counsel tells you to do -- do it, after you get that legal opinion in writing.

As stated in the "Introduction", no one person needs to perform all of the security-related tasks within the institution. But the Security Department is the logical function for coordinating the development, implementation, monitoring and correction of policies, procedures and practices that may affect the entire institution. The Security Department is one of the few functions that simply cannot afford to do the minimum amount of work necessary to "get by". Security is about doing what's necessary -- and often doing "what's necessary" involves extreme efforts from several people.

So -- for what else should the Security Department become responsible? These diverse -- but common -- examples are separated into the same five (5) industry-standard priorities of the Security Department addressed in "The Problem", and include:

- l Employees, insiders and institution-affiliated parties;
- l Customers, vendors and third-party service providers;
- l Facilities that the institution owns, manages, maintains or controls;
- l Assets that are both tangible and intangible; and

- Records and documents that exist in all forms, paper and electronic.

Employees, Insiders & Institution-Affiliated Parties

- Conducting background investigations -- and conducting all investigations concerning events, crimes, potential or suspected conflicts of interest and ethics issues;
- Developing and delivering training programs that address robbery, burglary and larceny -- and preparing a kidnap/hostage/extortion procedure;
- Hiring guards to protect employees at work who have been threatened or stalked;
- Supervising an "enforced leave policy" for all employees and insiders.

Customers, Vendors & Third-Party Service Providers

- Creating a system for maintaining the confidentiality of all customer records;
- Creating a system for maintaining the confidentiality of all employee records, such as job applications, results of drug screens, and criminal and credit checks;
- Interacting with your insurance representative in investigating customer-related, non-criminal acts that occur on the institution's premises -- such as auto collisions in the parking lot, "slips and falls" in the lobby and breeches of contract; and
- Conducting background investigations on selected commercial account applicants, vendors and third-party service providers.

Facilities That The Institution Owns, Manages, Maintains Or Controls

- Contracting with vendors to install, maintain and monitor alarm systems, surveillance cameras and access control devices;
- Continually investigating and recommending the adoption of contemporary security related technologies, such as "bandit barriers", security portals and biometric scanners;
- Making recommendations for solutions to facility design problems, using "Crime Prevention Through Environmental Design" (CPTED) principles; and
- Ensuring that all facilities contain appropriate emergency fire, medical and disaster recovery supplies and equipment.

Assets That Are Both Tangible & Intangible

- Applying for and monitoring of repayment for crime losses as ordered by the local probation department;
- Developing and implementing counterfeit currency and check practices;
- Conducting period risk assessments that involve real or perceived risks to each of the five (5) security-related priorities -- and that have been identified in the institution's Disaster Recovery Plan; and
- Working with the IT Manager and Auditor to develop and maintain an electronic inventory control system.

Records & Documents That Exist In All Forms, Paper & Electronic

- Developing and implementing effective safe deposit box security measures;
- Coordinating the filing of Suspicious Activity Reports with internal security reports and local law enforcement crime reports;
- Documenting all security training programs and maintaining other appropriate records -- including course outlines, lesson plans, workbook materials, training aids and instructor information; and
- Preparing and delivering a comprehensive Security Program Report to your Board of Directors.

The Security Officer also should become knowledgeable about regulations and practices that logically affect the Security Department, including (the):

Laws, Rules & Regulations

- All anti-money laundering regulations;
- All collections law and regulations;
- All criminal laws and facility safety ordinances in your state that are appropriate for the Security Department;
- All electronic funds transfer regulations;
- Americans With Disabilities Act;
- Bank Bribery Act;
- Bank Protection Act (or its equivalent for your industry);
- Bank Secrecy Act and Suspicious Activity Reports;
- Bank Service Company Act;
- Fair Credit Reporting Act;
- Financial Institution Recovery, Reform and Enforcement Act;
- Gramm-Leach-Bliley Act;
- Interagency Policy Statement on Contingency Planning;
- Polygraph Protection Act;
- Occupational Safety & Health Administration regulations;
- Regulation H (or its equivalent for your industry);
- Rights To Financial Privacy Act;
- Rules of Evidence (state and federal codes);
- Uniform Commercial Code;
- USA Patriot Act of 2002; and
- Workplace Illness & Injury Prevention Program regulations (applicable in several states).

Security Practices & Resources

- Conducting an investigation and interviewing conduct;
- Corporate investigative guidelines;
- Criminal justice components as they exist in your community (law enforcement, courts and corrections);
- Disciplinary actions and related policy and procedures;
- Domestic and workplace violence;
- Investigative report writing;
- Legal counsel and filing security-related reports;
- Searches of employees and customers;
- Sexual (or other) harassment or discrimination;
- Subpoenas and search warrants; and
- We-Tip or other anonymous reporting service.

Summary

Are you having a difficult time justifying the effort necessary to create an effective Security Program? Consider that your institution's ability to attract and retain qualified personnel and customers is directly related to your institution's professional image and reputation. This image is based upon trust and confidence -- and the perception of safety and soundness.

A professional reputation takes years to acquire, moments to destroy -- and an eternity to rebuild. Inappropriate and ineffective operational procedures used by your employees may destroy your institution's image -- and they are among the easiest operational mistakes to prevent. If your institution already has a Security Program, review it and assure yourself and your Board of Directors that it really meets your institution's needs. Because so much about the security function concerns safety -- employees' and other persons' -- simply meeting minimum regulatory requirements shouldn't be the goal.

Choose your institution's Security Officer carefully. Provide adequate training and supervision, grant sufficient power and authority to match the assigned responsibilities, and support his/her efforts to provide a safe and secure working environment. Becoming a professional -- and effective -- Security Officer requires special education, training and skills. It isn't a role for everyone. But if you approach the job with the right blend of enthusiasm, dedication and humor, you can easily become one of your institution's most valued assets.