Conducting a Library Facility Security Assessment Without Needing a Security Consultant

Dr. Steve Albrecht, PHR, CPP, BCC, CTM
619-990-2685
DrSteve@DrSteveAlbrecht.com

Why Assess?

Myths:	Realities:
"If we do this, we'll be 'on notice' to make changes."	You can make on-going changes, as time and budgets allow.
"It will increase our liability once we know about potential problems."	You are already at 100% liability the first day you open your library doors.

Our Mission

Any security change - related to new equipment, new policies, or additional personnel - should be measured by three issues:

Cost

Culture

Feasibility

We will call them "options," not "recommendations."

Assessment Team

Library stakeholders and walkthrough partners:

Library leadership; safety stakeholders.

Facilities management representatives.

Law Enforcement or Security representatives

Risk Management / Safety Officer

Knowledgeable managers and employees.

Access to buildings, rooms, policies, answers.

(Take pictures!)

Our Process

Security In-Depth: inside and out, people, policies

Perimeter Security Review

Facility Security Review / Access Control

HR, Security, Emergency, Evacuation Policy & Procedure Review

Information Security Review

Patron, Visitor, Vendor Procedures

Internal / External Theft Controls

Our Process

First-Aid Procedures

Fiduciary Instrument Controls

Police and Fire Department Interactions

Workplace Violence Response / Active Shooters

Emergency and Security Drills and Practice

Reporting Process

Implementation

Follow-up

Perimeter Security Review

- Walk the exterior of the building, including the parking lots. What is your overall impression?
- Graffiti, trash, homeless, problematic businesses nearby? Landscaping needs? Hazards?
- Area crime rates? Neighborhood "spillover" issues?
- Exterior building lights? Parking lot lights? Lot stairwells and elevators? (The need for a night visit.)
- Doors close and lock tightly? Hardware problems?
- Utility panels and shutoffs?
- Guards, barriers, proper signage, fencing, bollards?

Facility Security Review

Access Control, Access Control, Access Control!

- Multiple tenants? Shared-use facility? Landlord?
- Exterior door controls – key card readers, hard keys?
- Unsecured or secured separate lobby?
- Do employees come and go through the same doors as patrons? Exterior or interior cameras?
- Loading docks and warehouse doors? Roof access?
- Burglar or panic alarms? Fire suppression? Knox boxes?

HR, Security, Emergency, Evacuation Policy & Procedure Review

- Review all HR policies related to termination procedures, keys or key card and badge collections, network log offs.
- All security policies related to access control, visitor or vendor escorts, alarm codes, working after hours.
- All emergency and evacuation maps, policies, floor warden systems; for fire, bomb threats, earthquake, weather, and active shooters.

Information Security Review

- Meet with Library IT representatives about access control for server rooms, utility closets, mail rooms, copy rooms, use of asset tags.
- Discuss offsite backup procedures, emergency power, prevention of network intrusion, hacking, and related cyber threats.
- Review fire control rooms, equipment, procedures.
- Discuss updated PA system announcements.
- Review employee and patron hard-copy file protections.

Taxpayer, Visitor, Vendor Procedures

- Review or create a "Redbook" for Circulation Desk employees, with all emergency numbers, call trees, building plans, evacuation procedures.
- Review all visitor and vendor sign-in, badging, and escort procedures. Discuss trespass policies.
- Review where vendors work or wait: bullpens, lounges.
- Verify vendor key control and access: janitorial, landscaping, package deliveries, maintenance.
- Discuss patron, guest, visitor access issues.

Internal / External Theft Controls

- What are the most theft-sensitive items in the library? Tablets? PCs, laptops, projectors? Recyclable metals? Printer and office supplies? Software? Postage? Warehouse equipment?
- Review all inventory control and flow procedures, from delivery to shipping. Are certain items caged or stored under key?
- Discuss all past internal or external theft incidents.

First-Aid Procedures

- Review the locations of all first-aid kits, AED devices, (tourniquets), and sharps boxes.
- Review all first-aid training materials for CPR, bleeding, overdose, and minor injury responses.
- Remind all employees if they need to dial 9-1-1 or 9-9-1-1.
- Narcan training?

Fiduciary Instrument Controls

- Review the locations of all drop boxes, cash drawers, registers, safes, or vaults.
- Review all policies related to cash, check, and fiduciary instrument handling, blank checks, credit card machines, bank deposit procedures, petty cash disbursement, or the use of employee bank runs versus armored cars.
- Discuss internal audit procedures.

Police and Fire Department Interactions

- Verify the dispatch numbers for all local law enforcement (police and sheriff) and fire and EMS responders. Ask employees to put those numbers in their cell phones.
- Make sure building addresses are large and visible.
- Identify key law enforcement and fire personnel commanders for future support with drills, active shooter responses, or follow-up after police, fire, or EMS responses to the facility.

Workplace Violence Response

Review all workplace violence prevention policies: TROs, DV at work, new weapons possessions laws.

Review all workplace violence training materials for employee orientations or in-service programs.

Verify EAP contact information.

Discuss the formation of a Threat Assessment Team.

Discuss active shooter training, using the Run-Hide-Fight model. (DHS/City of Houston YouTube)

Identify potential safe room / shelter-in-place locations and make changes to door hardware and windows.

Emergency and Security Drills

Discuss the need for emergency, evacuation, and security-related drills with senior management. Schedule fire, weather, earthquake or active shooter drills at least once per year.

Meet with community first-responders to discuss these drills. Train all employees before all drills and debrief all employees after.

Create specific PA announcements, including, "There is an unusual incident in area X," for true active shooter situations.

Reporting Process

Date, time, location of site assessment, participants.

Executive Summary of key points, with photos.

Exterior and Interior Site Findings.

Security Improvement Suggestions (vendor neutral).

Appendices: Emergency, Evacuation, Active Shooter Procedures; Policy Improvements; Employee Training; Risks; Legal Issues; Targets; Threats.

Drafts, confidentiality, limited circulation, fact checks.

Security Officers

- In-house or contract? Armed? Powers of arrest?
- Review all posted orders for each guard position.
- Meet with guard contractor to update contracts, orders, create, or modify duties.
- Do guards serve a service function? Panic, burglar alarm, or open-door responses?
- How do they respond to an unbadged visitor in employee areas?
- Review guard equipment: pass keys, call tree lists, radios, time clocks.

Implementation

- Stakeholder meetings with City/County Department Heads.
- Report copies out on a need-to-have basis.
- Employee concerns or union issues?
- Review by Employee Safety Committee and City Attorney/County Counsel?
- Training classes, policy development and approval, equipment purchases and installations, capital improvements and physical facility changes?

Follow-up

- Don't write a report that dies on the shelf.
- Keep the stakeholder team on task and on time.
- Set hard deadlines for Department Head reviews.
- Set 30-day, 90-day, six months, and one-year follow-ups.
- Balance the need for changes with new incidents.
- Remember the Big Three: Cost, Culture, Feasibility.