ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org

Dear ASIS International Chapter Member:

The ASIS International Cultural Properties Council, House of Worship Committee (HOW) is pleased to share the enclosed documents with your local chapter. This information explains the Security Risk Analysis (SRA) process and represents the work of the ASIS HOW Committee, which I am honored to have served as Chair these past few years.

Prior to the SRA Process, ASIS members and other security professionals would assist HOW leaders improve security by conducting a basic security survey, followed by a report outlining steps for corrective action. In light of recent violence and terrorist attacks, the HOW committee felt a more robust and comprehensive process was required.

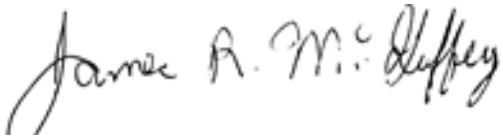
The SRA includes the security survey as part of a comprehensive process which allows leadership at houses of worship to identify critical assets requiring protection. Once these critical assets are identified, threats, hazards, and vulnerabilities are assessed, which are then evaluated using a numerical scale to determine level of consequence and probability of occurrence. After the level of consequence and probability are assessed, security strategies are selected by the key focus team to mitigate problems. The attached document, *Security Risk Analysis Process,* details this process and the benefits derived.

This process was tested by the Savannah Low Country Chapter, working with the Bluffton, South Carolina Police Department. Together, we hosted two three-hour seminars on a Saturday morning for approximately 80 clergy from various communities in S.C. and GA. These two events were covered by several TV stations and local reporters, and due to its success, other similar events were planned. These sort of community events will serve to benefit your ASIS Chapter and local communities.

As the instructor of this seminar, I was able to utilize the attached documents and process outlined to conduct a three-hour training that provided participants with the knowledge and ability to conduct an SRA at their own facility. The PowerPoint presentation we are sharing worked for me, but you may want to modify it to meet your own presentation style.

In closing, you may decide that you do not want to train numerous clergy as we did, and simply use the SRA Process and attachments to train one place of worship at a time; the choice is yours.

Sincerely,



Jim McGuffey, MA, CPP, PSP, PCI
ASIS Cultural Properties Council, HOW Committee Chair
ASIS Savannah International Savannah Low Country Chapter Chair

Enclosures:

- Houses of Worship, Security Risk Analysis Process *(white paper)*
- Actionable Steps to Improve Safety and Security at Your HOW
- Sample Letter for Workshop Participants, *(Microsoft Word file download)*
- Church Security Training, Security Risks Analysis, *(Microsoft PowerPoint download)*
- Updated SRA Checklist, *(separate file download)*

HOUSES OF WORSHIP
SECURITY RISK ANALYSIS PROCESS

An ASIS Council White Paper

PROJECT COMMITTEE MEMBERS

Jim McGuffey, CPP, PCI, PSP *(Chair)*

Phil Purpura, CPP

Doug Beaver

Christopher Provan

Dick Raisler

Jeffrey Berrett

Scott Watson

Doug Meacham

Carl Chinn

Johnie Mock

ASIS INTERNATIONAL® | Cultural Properties Council

Houses of Worship (HOW) are encouraged to follow an established process to ensure their assets are adequately protected. A "best practice" is to conduct a Security Risk Assessment (SRA) prior to making substantial changes to security processes. In the event a SRA cannot be conducted, there are steps listed at the end of this document that can be implemented to improve security.

Failing to conduct a SRA can often result in an inadequate and less than cost effective physical protection security system. It may also result in additional liability for the organization. The objective of this paper is to share a modified version of the SRA process, so that with guidance by a qualified security professional, house of worship leaders will be able to identify critical assets and assess threats and hazards. This information will help determine levels of undesirable consequences and probability of occurrence in order to select cost effective security strategies to mitigate risk. Unfortunately, many security practitioners continue to deal with significant threats and loss events using a reactionary approach without conducting a systematic security risk assessment, often implementing changes that are not well thought out.

A SRA must remain flexible. Church leadership, in most situations consists of volunteers working other jobs, so assembling a team to participate in a SRA can be challenging. If security professionals make the SRA process too cumbersome, it simply will not get done. While there are those HOW locations with very complex circumstances requiring substantially more time to complete an assessment and formulate a plan, the majority of locations will not require this sort of evaluation.

This is a summary document submitted by our ASIS International Cultural Properties Council HOW committee to be reviewed and continually improved. Our committee's goal is to turn this into a document that can be used by various ASIS International chapters in their communities to work with HOW to improve safety and security.

Often organizations conduct or request a security survey be done at their facility. A security survey will uncover some vulnerabilities, but it has numerous short-comings. The SRA process far exceeds benefits received from a security survey as a result of:

- Involving participation of HOW leaders and requiring support from top leadership. This ensures the end result is a plan that key people have formulated and feel they are part of the solution rather than one where there was little interaction on their part and no emotional involvement.
- Encompassing a holistic approach in identifying and mitigating vulnerabilities, and
- Ensuring that security strategies are carefully considered using a team approach which will ultimately result in superior protection of assets.

By including key facility participants and department managers, there is a better chance that more vulnerabilities will be discovered. Often what occurs in this sort of group effort, is one department manager learns of a past security incident and/or vulnerability that was not previously known. Without an open group discussion, such crucial pieces of information will go undocumented, resulting in an undiscovered vulnerability.

Selecting a Safety Focus Team

The SRA process begins with the HOW facility bringing together their key leadership, referred to as a Focus Team. This team is not to be confused with a security team, which will hopefully become one of the security strategies selected if a team is not already in place. The SRA Focus Team should consist of department heads from Management: Pastor(s), Finance, Admin, HR, IT, Security (if in place), Operations, Youth and Infant Care, and other key leaders deemed as beneficial to the SRA. Often with smaller size HOW, one person may perform several functions. Without key personnel being involved, the security plan that is developed will most likely fail.

The security professional leading the local ASIS Chapter in this process will spend approximately one hour with this Focus Team explaining the process and terms that people may not be familiar with, such as the difference between burglary, theft, and robbery.

Security Survey

Prior to training the Focus Team, the security professional will conduct a security survey with the person most familiar with day-to-day operations and outlay of the property. The security survey is a substantial part of the risk assessment process and is needed to evaluate vulnerabilities and learn the details of the facility, property, policies, procedures, personnel and technology utilized (or not utilized) within the existing Physical Protection System (PPS), or prior to formulating a PPS.

During a security survey, the security professional is working with a checklist to determine the effectiveness of the existing system, which are then shared with the SRA Focus Group.

The Focus Team will then identify and prioritize vital assets for protection, identify threats, hazards, and vulnerabilities; and develop cost effective security strategies to mitigate risk.

COLLECTING SITE INFORMATION:

Prior to the SRA and Focus Team training, valuable information is collected about the HOW facility. For larger organizations, several meetings at various stages within the SRA may be needed. For smaller HOW, this process can be completed within a day. The security plan will then be written by the ASIS person(s) orchestrating the SRA and forwarded to the SRA Group for execution.

The security survey and meetings with the Focus Team will serve to collect data on the physical and environmental conditions at the facility and property, past inspections, recent security and safety incidents, facility policies and procedures, existing technology, and facility operations.

Identifying and Prioritizing Vital Assets for Protection

Assets include people, property, information, and reputation—with people being the most important. It may not be possible or practical to protect all assets, therefore asset protection must be prioritized. Following are key considerations:

Our objective is to identify critical assets requiring protection and to prioritize, or value based on the consequence of loss. Consider cost of replacement, loss of productivity, loss of reputation, lowering of morale, historical value, and legal ramifications from loss of information and other factors deemed important.

1. People are always the most important asset, but some people require a higher level of protection. For example, children and infants require substantial focus to ensure adequate protection is provided.
2. Cost and ease of replacement.
3. Redundancy of assets. Are there other similar assets available? For example, a movie projector that is utilized daily might be listed under equipment. If there is not another projector that can be easily assessed, that piece of equipment becomes more critical to the mission as it relates to equipment.

Category of Asset	Example	Specific Threat or Hazard
People	Pastor	Assault
Property	Computer Room	Power Failure/Cyber Crime
Property	Main Facility	Vandalism
Information	Contributors Financial Information	Theft or Inadvertent Mistake
Processes	Automated Payroll/Payment	Theft

Table 1. Prioritize Assets (People, Property, Information, Processes, and Reputation)

ASSET EXAMPLES:

- **PEOPLE:** Pastors, employees, visitors, parishioners, youth groups, and infants in care of HOW.
- **PROPERTY/EQUIPMENT:** Facilities, land, equipment contained on the land and inside the facilities (consider historical value), computers, A/V equipment, artwork, money, organs, pianos, or anything of value or importance.
- **REPUTATION:** Often the reputation of a HOW is valued more than other valuable assets. In a publicly traded company, the market value can be substantially impacted, and within a HOW organization, membership growth can also be negatively impacted. Consider threats/inappropriate conduct that could significantly impact the reputation of your organization, such as sexual harassment, sexual affair or accusations of such conduct, and embezzlement. Consider the loss of reputation if a significant incident occurs, and it is obvious that something could have been (or should have been) in place to prevent or mitigate damage from occurrence.
- **INFORMATION:** Information stored on computers, inside file cabinets, or with a third party. Think about sensitive information that certain members within your organization have access to that would create legal or embarrassing ramifications if stolen or accidentally made public.
- **PROCESSES:** What are the processes used to run day-to-day operations that you want to protect? Payroll or other financial processes and Human Resource processes are examples.

Identifying and Prioritizing Threats and Hazards

Threats and hazards that could potentially impact critical assets are identified and prioritized. During this time, the Focus Team will consider the undesirable consequences of asset losses from each threat/hazard, and then determine the probability or likelihood of occurrence. A qualitative measurement of High, Medium, Low or numerical measurement 1 through 5 is used to measure value for each loss of consequence and probability of occurrence (with 5 being the highest value level assigned and 1 being to lowest). For example, a threat such as homicide resulting in loss of life which would be a 5 or High, where a theft might be valued as Low or 1.5 or 2.

Once each threat or undesirable consequence is identified for each critical asset, and the level of undesirable consequence is assigned, the probability of occurrence is then assessed. When determining probability, the Focus Team will consider recent past loss events at this HOW and similar facilities nearby, crime near the locale of facility, the PSP (physical protection system) and its various components (technology, policies and procedures, personnel) that exist or do not exist, and the opportunity for the threat to occur. For example, if there has been a recent homicide at a nearby HOW, and the HOW has no security program or PSP in place, the probability or likelihood of occurrence is most likely high or 4 or 5. A form is attached to assist in this process.

Other factors to consider when evaluating probability of occurrence are frequency of police patrols, isolation of the facility, and whether the exterior of facility presents a well-maintained appearance.

Following is a list of threats and hazards that other HOW have identified, listed in a format to help you rank and prioritize probability of occurrence. Your HOW may have other threats or hazards to consider.

PERSONAL CRIMES/SECURITY ISSUES

- Active Shooter
- Terrorist Activity
- Homicide
- Sexual assault
- Assault and battery
- Robbery
- Kidnapping of child by stranger or estranged family member
- Lost child
- Medical issues
- Infant injury while in care and custody of HOW

PROPERTY CRIMES/SECURITY ISSUES

- Burglary
- Vandalism
- Theft-external
- Theft-internal
- Embezzlement
- Arson
- Accidental fire
- Weather hazard

COMPUTER CRIMES/SECURITY ISSUES

- Cyber crime
- Lack of data back-up
- Viruses
- Power failure

OTHER THREATS/SECURITY ISSUES

- Picketing
- Improvised Explosives Devices (IEDs)
- Bomb threats
- Loss of reputation

Selecting Cost Effective Security Strategies

The Focus Team will then decide cost effective security strategies to apply to each threat or undesirable consequence to mitigate risk.

- Considerations in the security strategy selection process:
- Implementation cost
- Maintenance cost
- Impact from event
- Likelihood and opportunity to occur
- Likelihood of security strategy preventing threat
- Cost vs. benefit and sustainability

Following are security strategy options for consideration.

SECURITY STRATEGIES

1. Use of contract guards (armed/unarmed)
2. Use of proprietary guards (armed/unarmed)
3. Perimeter barriers CPTED (natural surveillance and boundary delineation)
4. Perimeter barriers (fence(s), gates, bollards, etc.)
5. Surveillance detection training
6. Improvised explosive preparedness (such as renting portable bollards, Jersey barriers, metal detectors

Policy and Procedure for security personnel and technology. Policies and procedures for but not limited to:

- Lighting
- CCTV
- Access control
- Motor vehicles
- Child care
- Youth trips
- Password protection
- Lost child
- Opening and closing of facility
- Key control

5. Increase security awareness (secure doors and windows/ environment awareness)
6. Enhanced pre-employment screening for volunteers
7. Enhanced pre-employment screening for paid staff
8. Security hardware (CCTV, alarm, access control), security film for doors/windows
9. Improved maintenance (cleanup, replacing burned-out bulbs, maintaining shrubbery, replacing burned out lights, etc.)
10. Lighting enhancement (motion lighting, enhanced lighting)
11. Annual inventory, ID/mark valuable items
12. Contingency planning and practice (disaster recovery plans for each probable disaster and loss event—floods, tornadoes, hurricanes, earth quake, fire, etc.)
13. Back-up generator
14. Medical training (for select personnel)
15. Secure additional insurance
16. Start a security program in cases where no security or safety program exists determine the cost and benefits of a security program consisting of paid and or volunteer members.

Implementation of Security Strategies

When implementing new strategies that are determined to be cost effective, it is important to make sure that there are no gaps between existing strategies and proposed strategies so that nothing is missed as it relates to protection efforts. Technology and policies and procedures must be reviewed to ensure that each does what is expected.

Maintenance Phase for Security Strategies

The maintenance phase is the most overlooked phase in the SRA process. It is imperative that all security strategies be managed, audited, and revised as needed to meet changing threats and vulnerabilities. There are numerous loss events that occur each day where state-of-the-art security systems and processes fail to detect, deter, deny, and respond to threats, simply because each new security strategy was not audited to ensue working order or revised to meet changing threats. Also, security strategies must be revised to meet changing threats.

Using the Vulnerability Analysis Form

A vulnerability analysis form is attached to be used for listing critical assets, determining threat/undesirable consequence, level of consequence, probability of occurrence, total score and security strategies.

Column 1: Prioritize Critical Assets

You will want to make multiple copies of this form since listing the various categories of assets and each threat that could impact a specific asset. For example, under the People Category, a HOW would have pastors, parishioners, employees, infants in their care, youth events, etc. Under the category of young children, for example, a few threats to consider might be injury, kidnapping, or lost child.

Column 2: Undesirable Consequences

List the threat or hazard that could negatively impact the asset identified.

Column 3: Impact of Undesirable Consequence

Follow the aforementioned instructions, using 5 for highest impact and 1 for least impact (you may use decimals). An example might be homicide, which most would agree is a 5, while vandalism might be a 2.5.

Column 4: Probability of Occurrence

Follow the aforementioned directions, using 5 for a threat or hazard most likely to occur and 1 least likely to occur.

Column 5: Total Score of columns 3 and 4

Add columns 3 and 4 and divide by 2. The higher scores will require immediate focus on protection efforts.

Column 6: Security Strategies

Use the number assigned to the appropriate security strategy. There will most likely be multiple security strategies assigned to mitigate each threat or hazard. For example, to mitigate risk to care of infants, strategies to consider might be 5, 6, 7, 8, 9, 10, or 16.

Column 7: Comments

A comment might be a point of clarification. Use back of form or another sheet for comments that you might want to recall at a later time.

Summary of Security Risk Assessment Process

1. Form SRA Focus Team
2. Conduct security survey (security checklist attached)
3. Review security survey with SRA Focus Team
4. Decide critical assets requiring protection (asset form attached)
5. Determine threats/undesirable consequence of loss that could impact each asset and assign a level such as H-M-L or 1-5
6. Determine probability of occurrence
7. Total score and focus immediate protection efforts on highest score area
8. Select cost effective security strategies
9. Develop security plan
10. Audit as deemed appropriate and revise as needed to meet changing threats.

Copyright © 2017 by ASIS International (ASIS). All rights reserved. Permission is hereby granted to individually download this document for personal use with acknowledgement of ASIS as the source. This document may not be sold, offered for sale, or otherwise used commercially.

The information presented in this document is the work of the author(s). The views and opinions expressed therein, or the positions advocated, may not necessarily reflect the views, opinions, or positions of ASIS or any ASIS member other than the author(s).

ASIS disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314
+1.703.519.6200
asisonline.org

ACTIONABLE STEPS TO IMPROVE SAFETY AND SECURITY AT YOUR HOW

There are actionable steps that can be taken which can have an immediate impact on improving safety and security at a house of worship (HOW) if a SRA cannot be performed in the near future.

1. Control access points. Use only entrances and exits as necessary. “Necessary” is the key word and should not be replaced with the word “convenient”.
2. Surveillance detection training.
3. Conduct background checks (criminal, employment, and references) and interviews for all paid staff and volunteers who are placed in positions of responsibility or trust. This includes the custodian, who is often the sole person inside a place of worship containing valuable assets.
4. Never allow staff or volunteers to work alone, especially at night. For custodians working alone regardless of time of day, doors should be locked to prevent entry.
5. Ensure opening and closing procedures are in place.
6. Make sure outside lighting is sufficient and shrubbery is properly maintained so there are no hiding places for assailants.
7. Make sure all doors and windows are secured when departing facility, and control these access points even when people are present.
8. Separate the duties of payables and receivables to reduce the risk of embezzlement.
9. Arrange your office space considering where infants are watched, money is counted, and other valuables are placed.
10. Make sure facility vehicles are properly maintained and a Motor Vehicle Check is run on drivers.
11. Ensure that the inside of the facility is properly lit at all times and fire exits are marked. If your budget allows, install back-up lighting in case of a power failure.
12. Install a burglar alarm, and make sure that it covers all access points, or at least the points where access must not occur. Basic alarm coverage is very inexpensive and can be improved upon as funding allows. An alarm response policy should be in place.
13. Have an emergency plan in place, and ensure it is periodically practiced and revised.
14. Ensure adequate fire extinguishers are placed in proper places throughout the facility and inspected annually. In most cases, the local fire departments regulate this safety practice.
15. Sensitive information should be identified and controlled (regardless if paper or electronic). Ensure information stored in desks or file cabinets are properly locked and secured when someone is not present. For electronic files, use and secure passwords. Treat a computer the same as a paper file by making sure the information cannot be accessed without permission.
16. Maintain an inventory of all expensive or easily stolen items and conduct a periodic audit to ensure all is present. Take photos and record serial numbers for electronic items and other items of significant value.

17. Provide security awareness training for paid staff and volunteers in positions of responsibility or trust. This training should include basic concepts of personal security, surveillance detection, first aid, child protection, domestic violence, and stalking awareness. Always have two adults with children and youth.
18. HOW members preparing to go on short-term overseas or domestic missions should receive a travel security briefing prior to departure.
19. A written log should be kept of all security related incidents. This log should be stored in a secure location and include: date, time, location, type of incident, who was involved, and a brief description of the incident.
20. Set up meetings with the local police and fire departments at least annually. These meetings will build relationships, set expectations, and allow for the exchange of information.
21. Include security and safety considerations when planning special events.
22. Monitor media outlets and social networks to ascertain what type of groups or events might impact the HOW.
23. Set up an inter-HOW security exchange in your community to share security-related information. Establish relationships with neighbors.
24. Multiple HOW in a community may consider selecting a nonprofit agency or a site with comprehensive security to be a centralized location for giving to destitute individuals and families. This would dissuade destitute individuals, and possibly offenders, from showing up randomly at multiple HOWs. And if they do, they can be directed to the appropriate nonprofit agency.
25. Consider protection for outside HVAC units that can be targeted for copper. Apply alarms with loud horns, fencing, cages with locks that can withstand bolt cutters, and CCTV.
26. Consider stained-glass window protection on the outside through shatter-resistant glazing.
27. Secure (i.e., bolt down) religious artifacts (e.g., statues) inside and outside to prevent theft.
28. Ensure crawlspace doors, roof access, and exterior electrical panels are locked.
29. Ensure bricks, ladders, or other items around the HOW are not available to be used by offenders.
30. Protect children from hazards by checking play areas, locking tools and chemicals away, and inspecting all areas.
31. Set a time period to change lock cores and keys.
32. Ensure fire, smoke, and carbon monoxide detectors are hardwired and backed up by batteries.
33. Check for trip and fall hazards on the premises.
34. Check the adequacy of snow and ice removal.

The House of Worship Committee also suggests a recently released book by Paula Ratliff, titled *Crime Prevention for Houses of Worship (2nd Edition)*, as a resource to provide you with a better understanding of the various crimes and with the preparation of policies and procedures to mitigate risk at your HOW.

This document was prepared by the Cultural Properties, House of Worship Committee during 2015 and submitted on February 15, 2016 for approval by ASIS International.

SAMPLE SRA WELCOME LETTER

ASIS International _____ Chapter is pleased to present the Security Risk Analysis SRA training session to help improve safety and security within our community Houses of Worship (HOW).

Founded in 1955, ASIS International leads the way for advanced and improved security performance through education, information, credentials, industry standards and guidelines, advocacy, and more. The scope of our professional development and global networking opportunities is unmatched. Our members within the public and private sectors have full and exclusive access to the information resources required to keep pace with security issues and concerns, as well as strategies for mitigating risk to people, property, and information. Additionally, and most importantly, our members have the ability to build and sustain long-term industry relationships within our vast global network of professionals.

Our ASIS International and _____ Chapter members are Law Enforcement, Military and private security professionals working together to share best practices to keep our communities secure.

ASIS International has a wealth of resources on it's website for both members and non-members. One such resource is a newly released book release titled *Crime Prevention for Houses of Worship* by Paula L. Ratliff. This book will be a great supplement to enhance your workshop experience today.

Please contact me at _____ for additional information regarding ASIS International and our local ASIS Chapter. We hope that you will consider joining ASIS International and being part of our local _____ Chapter.

We also invite you to attend one of our monthly lunch meetings as announced on our web site several weeks prior to each meeting.

Thank you for your participation in our timely training session today!

CHAPTER CHAIR SIGNATURE

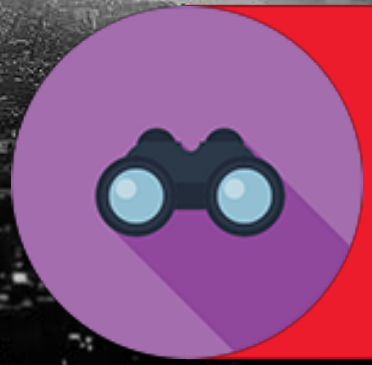
THE SECURITY RISK ANALYSIS

by the Savannah Low Country Chapter and Bluffton Police Department

A Community Partnership to Improve Security for Houses of Worship

Instructor: Jim McGuffey, CPP, PCI, PSP

ASIS INTERNATIONAL
Advancing Security Worldwide®



WHEN EVIL WALKS IN: PROTECTING GOD'S PEOPLE

http://abc7chicago.com/religion/when-evil-walks-in-protecting-gods-people/1082130/

DISCUSSION POINTS

- Security Risk Analysis Process
- Benefits of a Security Program

REASON *NOT* TO HAVE SECURITY PROGRAM

- Knee-Jerk Reaction to a Violent Crime or Shooting

Consider a security program for the so many other benefits it can provide

PRIOR TO SECURITY PROGRAM

- Conduct analysis prior to purchasing equipment, starting a security program, or changing major process/policy in existing program
- Will also help to understand benefits of security program

RISK MITIGATION OPTIONS

- Ignore
- Risk Transference (Insurance)
- Accept and Mitigate

SRA PROCESS

- Considers critical assets
- Prioritizes protection efforts of critical assets
- Assesses threats and vulnerabilities
- Evaluates the likelihood of threats occurring
- Evaluates impact of threats
- Determines cost-effective security strategies

SRA STEPS

1. Security Survey
2. Safety Focus Tam
3. Critical Assets
4. Threats and Hazards
5. Level of Consequence
6. Opportunity to Occur
7. Security Strategies
8. Gap Analysis
9. Maintenance

SECURITY SURVEY

Security professional conducts the survey with person most knowledgeable of operations, property, and day-to-day operations.

SECURITY SURVEY BASICS

- Past Incidents
- Police Reports
- Opening/Closing
- Emergency Response
- AHJ Relationships
- Financial Controls
- Key Control
- Controversial Issues
- Computer Control
- Computer Protection
- Local Events
- Youth Programs
- Child Care
- Background Checks
- Burglar Alarm
- Fire Alarm

SECURITY SURVEY — PERIMETER

(Become the Adversary)

- Lighting Around Facility (hiding places)
- Parking Lot Lighting and Distance (night time)
- Shrubbery/Trees (hiding places)
- Doors/Frames/Locks/Hinges/Closure
- Windows and Access Points

SECURITY SURVEY — PERIMETER

- Visibility (inside out - outside in)
- Visibility for Police and Others Viewing
- Secluded/Rural Location
- Roof (flat roofs of more concern)
- Condition of Facility (tinder box)
- Backup Generator (mega-size operations)

SECURITY SURVEY — INTERIOR

- Door Control
- Lighting (entrance/exits/hallways)
- Backup Lighting (entrance/exits/hallways)
- Child/Infant Care Areas (access)
- Burglar Alarm (sensor coverage)
- General Safety (exposed wiring/chemical storage/broken window latches)

SECURITY SURVEY — ADMIN

- Personnel Records/Sensitive Data (controls)
- Audit Process for Fixed Assets
- Audit of Payables and Receivables
- ID for High-Value Items
- Reporting of Incidents (internally - AHJ)

SELECT SAFETY FOCUS TEAM

- Senior Pastor
- Key Department Heads
  - ❑ Finance
  - ❑ IT
  - ❑ Youth Pastor
  - ❑ Maintenance
  - ❑ Admin
  - ❑ Security

SELECT CRITICAL ASSETS PROTECTING

- Assets are People, Property, Reputation, and Information (tangible or intangible)
- People Most Important
- High Value Assets, Artwork, Etc.
- Replacement Difficulty and Cost
- Information Systems: Payroll, Contributors, Hiring Data
- Most Impact on Revenue Loss and Reputation

IDENTIFY THREATS

Sources for Identifying Criminal Threats

- Local Police Crime Stats
- UCR for Your Municipality
- Internal Records
  (legal actions, incidents)
- Other Churches
- Professional Groups
- CAP Index

THREATS

- Assault
- Sexual Assault
- Computer Crime
- Information Leakage
- Child Molestation
- Lost Child
- Child Kidnapping
- Domestic Dispute
- Vandalism
- Burglary
- Theft
- Fire (Act of God)
- Fire (Accidental)
- Arson
- Embezzlement
- Picketing
- Bomb Threat
- Terrorist Attack – IED's
- Active Shooter
- Drug Abuse
- Misuse of Computers
- Hurricane/Weather Issues
- Power Failure

LIKELIHOOD OF OCCURRENCE

Considerations When Evaluating Likelihood

- Educated guess based upon historical data
- Socio-economic (crime, poverty, gangs)
- Police response/patrol/closeness to PD
- High profile stances on issues
- Closeness to major highways
- Secluded area

LIKELIHOOD OF OCCURRENCE

- Inadequate or no security policies, procedures, or systems in place to deter or mitigate
- Weaknesses Within Your Operation
- Ease of criminal committing act

Rank 1 – 5 (1 least likely; 5 most likely)

IMPACT/LEVEL OF CONSEQUENCE THREATS/HAZARDS

- Impact to Church
- Impact to Visitors, Individuals, Yourself
- Impact can be Psychological, Monetary, Personal, Long Term, Short-Term, etc.

Rank 1 – 5 (1 low impact; 5 high impact)

SECURITY STRATEGIES

Designed to

DETER

DETECT

DELAY

DENY

RESPOND TO

and

RECOVER

from Security Event

SECURITY STRATEGY CONSIDERATIONS

- Implementation Cost
- Maintenance Cost
- Impact/Consequence from Threat or Hazard
- Likelihood of Preventing Threats
- Attractiveness of Asset
- Does Cost Exceed Benefit

SECURITY STRATEGIES

- Procedural (openings and closings)
- Policies (key control, hiring) (technology and people)
- Increase Awareness (secure doors and windows)
- Maintenance (shrubbery, bulbs, clean-up)
- Pre-employment Screening
- Modify Control Points When Open (doors)
- Fencing/Barriers/No Trespassing Signs
- Burglar Alarm
- Lighting Enhancement
- Contingency Plans

NOTE:
All security strategies must be monitored and revised as needed to meet changing conditions

Threats are not static!

SECURITY STRATEGIES

- Surveillance Detection Training
- Conduct Inventory Annually, Mark Valuables
- Security Film (doors and windows)
- Access Control
- CCTV
- Back-up Generator
- Emergency Lighting
- IED Evaluation (consider plan to rent portable bollards and Jersey Barriers if needed)

MEGA SIZE WEEKDAY OPERATIONS

- ID Badge (employee visitors)
- Sign In/Control Log

LET'S SELECT SECURITY STRATEGIES

Use Vulnerability Analysis Form

No single security strategy will prevent all threats or risks from occurring at your place of worship. It is best to create layers of cost-effective protection known as site hardening or in-depth protection.

SECURITY STRATEGY MAINTENANCE

- Risk is never static!
- Security strategies must be re-visited
- Training ongoing
- Security survey annually
- Processes and procedures audited
- Ongoing management portion of the SRA Process

CORNERSTONES OF A SECURITY PROGRAM

- Leadership
- Hiring
- Auditing
- Revise Security Strategies as needed
- Ongoing Training
- Annual Security Survey

OBTAIN LEADERSHIP APPROVAL

- “Buy-in” support and participative leadership from pastor and other leaders
- Security analysis will help finalize written plan for cost, requirements, and strategies

SECURITY PROGRAM BENEFITS

- Handle Medical Events
- Prevention, Issues of Concern, Active Shooter
- Focus on Vandalism and Burglary (76%)
- Audit of High-Value Items
- Handle Special Events
- Sense of Security for New Members with Childcare, especially Infant Care
- Continual Focus on Vulnerabilities and Changing Threats
- A Chance to Serve a Special Group

DETERMINE AVAILABLE RESOURCES

- Prior or active security or law enforcement, firefighters, EMTs, and those with a real interest to be volunteers
- Insurance Company
- Local Police/Fire Department/EMT
  - Use for Training
  - Build Relationships
  - Good Intelligence Sources

MAJOR CHANGES

- Check with insurance company and AHJ for adding programs such as firearms or labeling as security program
- Some states and municipalities require training even if no firearms by simply referring to team as security team

SECURITY TEAM MEMBER ATTRIBUTES

Crucial Attributes

- Commitment
- People Skills
- Integrity
- Experience Can Be Achieved!

LEADERSHIP

Select member with proven leadership skills (motivational, able to develop others) who plans on being with you for a while

TEAM MEMBER QUALIFICATIONS

- Criminal Background Check
- Prior Employment Check
- Church Member for Six (6) Months
- Able to Meet Training Commitments
- For Those with Driving Responsibility: MVR
- Set Driving Standards—Violations/Accidents

A WARNING ON BACKGROUND CHECKS

- Protect information in handling and storing
- Just because no record exists ……
- Suggest someone skilled in interviewing
- Recheck every three (3) years on criminal; annually for drivers

OTHER ITEMS

Required Items

- Operations Manual, Incident Reports, Guidelines
- Contingency Plans

Other Considerations

- Uniforms or I.D. Badges
- Cell Phones/Two-Way Radios
- Areas and Times of Coverage
- Duties

SAFETY TEAM TRAINING TOPICS

Training Based Upon Security Risk Analysis

- Medical Emergencies
- Basic First Aid
- Lost Child
- Irate Person (de-escalation training)
- Emergency Evacuation
- Active Shooter

ONGOING RESOURCES

- ASIS Savannah Low Country Chapter
- Law Enforcement
- EMTs
- Fire Department
- Insurance Company

THANK YOU

A.C.E. Security Consultants House of Worship Checklist

(Revised November 4, 2016. Jim McGuffey)

House of Worship Check List	Location	Location	Location	Location	Comments
Employee/Parishioner Awareness					
List Existing Programs					
Other:					
Law Enforcement Relations					
Established relationship?					
Other:					
Surveillance Detection (SD)					
Are Red and Green Zones Established?					
Are key people trained in SD?					
Other:					
Improvised Explosive Devices (IED)					
Are vendors on call for portable Jersey barriers?					
Is staff trained in IED awareness					
Are staff trained in suicide bomb awareness?					
Are staff trained in VBIED security strategies?					
Other:					
Exterior Doors					
Do exterior doors provide notification when left open or accessed?					
Are exterior doors metal or solid material with adequate locks?					
Are hinge-pins on exterior doors protected?					
Are emergency doors equipped with panic hardware?					
If alarmed, does it indicate on alarm panel that door is open?					
If window, is security film or bars needed?					
Do exterior doors have peepholes?					
Is there access control on exterior doors and CCTV?					
Is CCTV video activity recorded with periodic backups?					
Is there a UPS system integrated into the access control system?					
Other:					
Windows					
Are windows able to be secured? For those requiring additional protection, consider adding security film to strengthen and an alarm sensor.					

Consider strength of glass; distance from hiding places and locations allowing access into special areas.					
Are any windows alarmed?					
Are hurricane windows needed?					
Other:					
Facility Access via Tunnels, HVAC, etc.					
Are there unusual openings such as manholes, underground tunnels, skylights, ventilator shafts, roof latches protected? How?					
Other:					
Perimeter Security					
Are shrubs and trees trimmed back around facility to prevent hiding places?					
Are parking lots and facility visible from the street?					
Does parking lot have potholes or other unsafe conditions?					
Review for CPTED—graffitti, line of sight, cleanliness, etc.					
Is there adequate protection during night services for those arriving and departing?					
During hours of darkness when parties depart, is there a procedure to ensure elderly and others are escorted to car and people depart in groups?					
Is there a perimeter fence? If yes, is it in good repair with working gates that can be secured?					
Are 'No Trespassing' signs posted?					
Do police routinely patrol the area?					
Will the appearance of the facility and landscape be viewed as being cared for?					
Are all exterior doors locked and alarmed at closing?					
Are exterior facility, pathways and parking lot lamps adequate?					
Are motion sensor lights in place?					
Are lights checked periodically for proper operation?					
Are access points on roof or other parts of facility, such as tunnels, alarmed or otherwise secured?					
Other:					
Interior Lighting					
Adequate for entrances/hallways/exits?					
Is there battery back-up lighting? How many hours?					
Other:					

Alarm System					
If alarmed, do sensors cover required areas for protection?					
How is alarm system monitored?					
Is there an updated contact list and are those on the list trained in alarm response?					
Review incidents, maintenance agreements, and coverage.					
Other:					
Access Control					
How is access controlled?					
Is there a receptionist or control person in place at entrance?					
Are ID badges issued and worn by employees?					
Who controls ID badges if used?					
Are visitors issued badges during week days? (Not referring to those attending church services)					
Other:					
Bomb Threats					
Are procedures in place to deal with a bomb threat?					
Other:					
CCTV					
Review maintenance program					
Are access points, money and sensitive information rooms, and rooms where infants and youth are cared for monitored via CCTV?					
Is system adequate? (clarity, lighting, recognition, storage)					
Does system cover inside and outside area?					
Is system adequately protected from unauthorized access?					
Can video be reviewed off premise?					
Is CCTV system integrated with access control and alarm system?					
Is video reviewed daily to ensure clarity, correct time, and that it is recording?					
Check video storage and backup.					
Are cameras protected with proper housing against vandalism, unauthorized movement, weather elements?					
Is there a review form requiring date and time of daily review and initials?					
Other:					
Trash					
Is sensitive information shredded or properly disposed of?					
Other:					

Emergency Plans					
Are emergency plans in place for all reasonable events?					
Date when plan last rehearsed.					
Other:					
Financial Controls					
Petty Cash: Are adequate controls in place? Receipts/audits/access					
Is a safe used? Is it adequately secured and bolted to floor if less than 750 lbs.?					
Are deposits made with safety in mind?					
Collections: Review dual control and deposit method.					
Is inventory such as laptops, audio equipment and other valuables marked to aid in the recovery process?					
Are assets such as chairs, tables that are not marked counted annually or as needed to ensure that none are missing?					
Does inventory sheet include book value, serial # or other ID marking, and location of item?					
Are there photos of substantial valued items for recovery purposes?					
How often are inventory audits performed?					
Other:					
Payables and Receivables					
Are these functions controlled by different staff?					
Does each function have written policies for controls and audits?					
How often are audits performed?					
Are two signatures required on checks over a certain dollar amount?					
Other:					
Openings and Closings of Facility					
Are opening procedures in place?					
Are closing procedures in place?					
Other:					
Contractors and Vendors					
Review process for vetting vendors to ensure properly licensed and insured. When working around infants and children a more intensive vetting needs to occur.					
Are vendors monitored?					
Other:					

Hiring Policy					
Are background checks to include prior employment done for those involved in child care and youth programs?					
Are background checks done on those involved in financial programs?					
Are interviews conducted by a trained interviewer to avoid illegal questions and to look for, evaluate and respond to responses that may be indicative of deception?					
Are financial checks and background checks done in accordance with the FCRA and State law?					
Do background checks consist of National Criminal Records Checks and past employers? (volunteer and paid)					
Other:					
Safety					
Are there adequate number of fire extinguishers that are marked and inspected annually?					
Are emergency doors equipped with panic hardware?					
Are emergency exits marked and posted as required by AHJ?					
Is there emergency lighting?					
Are emergency evacuation maps posted?					
If required, is MSDA available and properly displayed and maintained, and training conducted and documented?					
Does facility have and practice emergency plans?					
Are emergency exits free of obstructions?					
Is the facility inspected for safety hazards such as loose or unsafe wiring; area safe from slip and falls?					
Is there a safety and security check list that is managed and maintained if needed?					
Is there a back-up generator? How many power failures in past year?					
Are gasoline cans and other flammable items properly stored?					
Are water, electrical, heat, as utilities secured?					
Other:					
Issues that Might Attract Dissidents					
Is church involved with human rights issues such as abortion and gay rights?					
Are there such events occurring in the neighborhood?					
Have there been incidents in the recent years?					
Other:					

Record Storage and Maintenance					
Are sensitive files maintained inside a solid heat resistant fire cabinet which is secured on need to access basis?					
Is access to these room(s) kept to a minimum (need to access basis)?					
Does the room use key or electronic access?					
Is there CCTV coverage?					
Are those handling sensitive information trained in compliance with legal requirements?					
Is office door and cabinet secured when no one is present in room?					
Other:					
Cyber Security					
Are laptops containing sensitive data taken off site?					
Are all computers adequately secured?					
Is information backed up as needed in case of power failure, virus attacks or other issues?					
Are computers password protected?					
Is there adequate virus protection and a firewall in place?					
If using cloud storage, has due diligence been done to ensure reliability and adequate notification and coverage if a breech occurs?					
Others:					
Vehicle Management					
Is there a policy in place regarding violations and accidents for drivers operating church vehicles?					
Are vehicles properly maintained, a record of maintenance reviewed, and conditions requiring action acted upon immediately?					
Are vehicles checked daily by those using them to ensure that lights, brakes, and other safety features are in working order; and if not, a report is made on safety issues and immediately corrected?					
Are MVRs ran on drivers annually?					
Are pre- and post inspection reports used? And are reported safety issues monitored and corrected?					
Are all drivers qualified with a driving test, and is training on-going?					
Is there a policy in place for violations and accidents?					
Other:					
Mailroom					
Is there a mail room policy that describes procedures for handling suspicious mail?					

Are people handling mail trained to recognize, handle and report suspicious mail from USPS, FEDEx, UPS or other services?					
Is there a containment bin to place suspicious mail?					
Other:					
Key Control					
Is there a key control policy in place that requires on-going audits to ensure compliance?					
Are keys assigned to only those personnel with a specific need?					
Are keys stamped with 'Do Not Duplicate'?					
Is a record of assignment maintained?					
Are master keys issued to only those with a specific need?					
Is someone assigned to manage key control?					
Other:					
Contractors and Vendors					
Are contractors issued keys and badges? How are they controlled?					
Are contractors checked for Worker's Comp insurance, and background checks if working around youth or valuables?					
Other:					
Emergency Management and Business Continuity Planning					
Are plans in place to ensure an orderly process during the recovery stage?					
Are evacuation plans practiced annually or as needed?					
Is ther an up-to-date vendor emergency contact list and employee list?					
Do you work with local officials in the planning and practice stages to develop a working relationship and ensure adequate planning is done?					
Is there a plan in place to address a lost or missing child?					
Does your business continuity plan provide for leadership succession and a place to meet during the recovery process?					
Are communications in place to notify the public and members regarding updates?					
Is there a copy of facility blue prints identifying water, heating, gas, electrical controls that can be shared with emergency providers?					
Other:					

Youth and Child Care					
Are there policies and procedures to ensure adequate child care and youth protection during on- and offsite activities?					
Are doors and windows adequately protected where child care occurs?					
Are care providers trained in child care as it relates to medical emergencies, release to proper custodian, securing the room in case of a security incident, reporting incidents?					
Are background checks and past employer checks conducted on both paid and volunteer staff?					
Are policies existing and monitored to ensure adequate protection for youth during field trips?					
Is there CCTV coverage for child care rooms?					
Is access controlled for rooms where youth activities occur and are sign out controls in place?					
Are incidents involving child and youth care documented and reported to all those concerned to include law enforcement?					
Other:					
Miscellaneous					
Is there a security program in place? If so, describe it on separate page.					
Are there nearby facilities that can pose a threat such as abandoned buildings, chemical plants?					
Is this area prone to flooding, tornadoes, hurricanes, or other natural disasters?					
If security strategies and emergency plans exist, are they managed and revised as needed to meet changing threats, vulnerabilities and hazards?					
Are playgrounds safe and monitored? Is CPTED in place? (no trespassing signage and areas clearly obvious that public should not wander on to)					
Is there a public address system in place?					
Are security and safety incidents reported to staff and, if appropriate, to police?					
Do employees travel overseas and, if so, is there adequate security training that occurs?					
Other:					