Addendum to Houses of Worship: Security Risk Analysis Process white paper, May 2017

INSIDER THREATS TO HOUSES OF WORSHIP

HOUSES OF WORSHIP COMMITTEE CHAIR:

Jim McGuffey, CPP, PCI, PSP

CONTRIBUTING MEMBERS:

Paula L. Ratliff

Douglas M. Meacham, CRM

Alistair Calton

Philip P. Purpura, CPP

Dick Raisler

ASIS INTERNATIONAL® | Cultural Properties Council

"Managing a house of worship (HOW) like a business" is a cliché that many religious leaders aren't willing to embrace as a component of their management style. Research supports that most churches are governed by volunteers who step into a leadership role with merely a willing attitude to serve and a handshake. Religious leaders are hesitant to question a person's faith, background, and intentions. Perhaps it is a pious attitude of, "I'm a good judge of character." Paula Ratliff, author of ASIS International best seller, Crime Prevention for Houses of Worship, 2nd ed., stated, "in my twenty plus years of research, I have never heard a pastor say, 'Well, we always suspected something'." Instead, religious leaders are interviewed on television and the narrative is usually the same. He was a "good person" and "we just can't believe this happened to us."

HOWs can provide a location for criminal acts, whether committed by persons who are known or unknown--be it a total random act, or one that is planned to the minute detail. One of the more recent murders occurred on April 18, 2016, in Midlothian, Texas, when Missy Bevers arrived at the HOW early in the morning to teach an exercise class. Prior to her arrival, a perpetrator, dressed in what appeared to be SWAT gear with the word "Police" on the back of his/her shirt, entered the church. Security cameras captured the killer's entrance and movement in the building, but the clothing, padding, helmet, etc., concealed positive identification. Little evidence was left, and as of this writing, no arrests have been made. Police, thus far, have not released any images of the struggle that pursued as Missy suffered fatal puncture wounds to her head and chest. It is unknown whether this was a burglary or a direct hit committed by a stranger or an acquaintance.

However, offenses such as embezzlement, theft, and sex crimes are generally committed by known persons. A security risk assessment (SRA) must be completed to determine vital assets (refer to Houses of Worship Security Risk Analysis Process white paper). Once the SRA has been completed, consideration must be given to who has access to the most vital assets of the HOW. Therefore, it is important that administrators (senior pastor, HR director, facilities director, school/childcare director, CFO, and IT director) carefully review the responsibilities of each volunteer and staff person within the congregation. An important part of this process is that it causes HOW leadership to think about threats to their organization—Insider Threats.

1. Make a list of each person, their title, and what they have access to within the HOW.

2. Establish a file on each staff person to include their application, credit report, and background check. Individuals holding volunteer positions should also have the same reports in their files.

    a. Applications should ask about prior criminal convictions.
    b. Consideration should be given to youth who may have criminal history that has been sealed.

3. Determine who has access to money, financial information, IT systems, pastoral/clergy personal information, and children.

4. Determine the level of threat, i.e., high, medium, and low (see chart below).

5. Develop a plan and a watchful eye in any area identified with a high or medium rating.

6. Review annually or when positions or staff responsibilities change.

Insider Threats for Embezzlement, Theft, and Sex Crimes

What can be done to reduce the level of "Insider Threats?" A step in the right direction is to "think" that your congregation and administrative structure could potentially pose a threat under certain conditions. It is important to remain vigilant and to identify the "threat" areas. While the chart lists only three criminal actions, we know that there are others to consider.

Any position/title with a rating of high or medium needs to be of concern. The above chart is an example of an evaluation of staff members who could potentially pose a threat simply because of their positions.

Based on these assessments, identify ways to lower the threat. For example, the pastor has access to everything within the church. He/she could embezzle money at any time; however, if a policy is established that two people must sign off on checks and the books must be reconciled by a third party, then the opportunity to embezzle is greatly reduced. Creating a focus on procedures in various high-risk areas will help decrease the chance of internal loss.

A childcare director has direct access to children. Anyone in this position should have a thorough background investigation to ensure there was no previous concerns with children. A way to reduce the threat and protect both the church and the director is to install security cameras (consider privacy laws for HOW jurisdiction). These files should be retained for many years as victims of sexual crimes often do not come forward immediately. Additionally, HOWs should consider a two-deep policy (never only one adult with one child or challenged individual), windows to view into rooms, Dutch doors, training videos on protecting children, and signed statements that attendees comply with policies and procedures (may be required by insurer).

This type of assessment should be completed for every position in your congregation and include as many criminal categories as possible. Additionally, it should be reviewed when staffing changes are made or significant policies updated. For example, the custodian may be filling in for the treasurer who is on sick leave. That change is giving him/her access to money and the opportunity to commit fraud. Perhaps the youth pastor has requested a separate checking account for the youth funds, or has started conducting counseling sessions behind closed doors, or is actively planning a camping trip.

Position/Title	Access to Embezzle	Collusion Opportunity	Access to Financial/IT Information	Collusion Opportunity	Sex Crimes with Children or Adults	Collusion Opportunity
Pastor/Clergy	High	High	High	Medium	High	High
Youth Pastor	Medium	High	High	Medium	High	High
Secretary	High	High	High	High	Low	Low
Treasurer	High	High	High	High	Low	Low
Custodian	Low	Low	Low	Low	High	High
Child Care Director	Low	Medium	Medium	Medium	High	High
Operations Manager	Medium	High	High	High	Medium	Medium

Each of these threats can be reduced with proactive approaches. For example, policy should prohibit separate checking accounts. The secretary/treasurer should monitor all expenditures and submit monthly reconciliation reports with oversight by a CPA and/or other board members. Closed door counseling sessions should be prohibited unless the office has a window that is within viewing sight of others in the HOW. Logs of meetings (calendars) and notes should be retained for several years. Camping trips and sleepovers, if allowed, should be supervised to ensure safety, security, and that reputations are preserved.

Rules and protocols should have buy-in and an ongoing commitment by leadership and be reviewed with staff on a regular basis. Additionally, new staff and volunteers joining the HOW should be trained on the rules and protocols. There should also be some level of repercussion for not following rules and protocols. As with no leadership buy-in, if there are no repercussions, staff and volunteers will view the rules and protocols as lax.

Additionally, consideration should be given to introducing staff and volunteers to the enterprise risk management concept while in training. Managing risk including the insider threat is the responsibility of all staff and volunteers whether there is one HOW campus or twenty.

Each activity should be reviewed for potential threats—both in and outside. Consider your vulnerable activities and work to reduce the potential. If you fear someone from the outside may come in, then install cameras, hire a security firm, put security barriers in place. If you have an insider threat, then work to reduce the threat.

The key to reducing and/or avoiding criminal activity is to reduce the risks and the opportunity. Acknowledging that there is a potential for an "insider" to commit a crime is the first step toward a safe environment.

As HOWs become more and more reliant on cyber technology, significant consideration should be given to insider cybercrime. HOWs are not only reliant on technology for their day-to-day functioning, but private information on congregants is also gathered. HOWs need to be proactive on not only determining what their greatest cyber assets are and protecting them, but also on developing rules and procedures for staff and volunteers on technology usage. Through training and education of IT rules and protocols, HOW leadership can reduce the probability insider cybercrime will occur and mitigate risk.

ASIS INTERNATIONAL
Advancing Security Worldwide®

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