Volume 3, Issue 5
May 2021

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level: Severe

FB-ISAO has assessed the general Physical Threat Level for US Faith-Based Organizations as **"SEVERE."** As per FB-ISAO's definitions of the Physical Threat Levels, **"SEVERE"** means that an event is highly likely.

Please note that the Pandemic Threat Level has been lowered to ELEVATED.

FB-ISAO Cyber Threat Level: Guarded

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as **"GUARDED."** As per FB-ISAO's definitions of the Cyber Threat Levels, **"GUARDED"** means FB-ISAO is unaware of any specific events, but a general risk of incidents exists.

Stories

New Membership Level Offering, Page 1

Averting Targeted School Violence, Page 2

Spotlight: Ransomware, Page 2

Upcoming Events, Page 2

FB-ISAO Newsletter

New Membership Level Offering

Basic Plus

The Faith-Based Information Sharing and Analysis Organization (FB-ISAO) is a 501(c)(3) non-profit organization with a mission of providing members with **information**, **analysis**, and **capabilities** to help **reduce risk** while enhancing **preparedness, security, and resilience**. We are an all-faiths and all-hazards information sharing organization.

As is the natural trajectory of many information sharing organizations / groups, the foundational operational mode is one-way information sharing. That is, the organization shares information with its members. As trust builds and the organization evolves, two-way information sharing begins. In this scenario, members share information back. The golden nugget for any information sharing organization is collaboration where information flows in a circular direction. This can be powerful especially when our government and law enforcement partners are part of the process as well.

In the past year, and for the purpose of increasing collaboration, FB-ISAO has hosted many events. Our events are purposefully collaborative. We believe in spending less time talking **at** our members and more time talking **with** our members. To that effect, many of our events are focused on the members themselves participating in the discussion. Some of the events we have held include:

- A grants town hall
- A discussion on the Mitigating Attacks on Houses of Worship Security Guide
- A review of the Poway Shooting incident
- Monthly Threat Briefs on various topics to include
    - How to safely observe religious commemorations during a pandemic
    - Protests and their effect on faith-based organizations
    - 5 Terrorism Trends to Watch in 2021: violence against faith-based institutions

Since June of 2018, FB-ISAO has been mainly focused on physical threats, however, since we are an all-hazards information sharing group, we will be introducing a new series of events focused on cyber education in June / July of 2021.

The events above have been inclusive of all our members – even those at our no-cost level. Starting in July 2021, we are adding another membership level. That membership level will be known as Basic Plus and will cost $99.00 per year. Members at our no-cost level of membership will be able to continue to receive their current benefits, but they will be required to upgrade their membership if they would like to attend any of our events. Members at our standard, professional and law enforcement levels of membership are unaffected by this change. An official notice will go out to all our members.

Now is the time to start planning for this change! During the month of July 2021, for the cost of upgrading to the Basic Plus level of membership ($99), FB-ISAO will step-up the member to the standard level of membership. At our standard level of membership, members can access Information Sharing Communities as well as events. Learn more about Information Sharing Communities. Details to follow.

FB-ISAO Advisory Board

Get to Know the Board of Advisors

Contact Us

Company Name
FB-ISAO

Email
Info@faithbased-isao.org

Website
www.faithbased-isao.org

Not Yet a Member of FB-ISAO?

How to join…

Not Yet on FB-ISAO Slack - You Need to Be!

Write to membership

Upcoming FB-ISAO Events

Monthly Threat Brief	25 May
Member On-Boarding	21 May
Hostile Event Preparedness Workshops in PA	March, April and June

Averting Targeted School Violence

On 30 March, the U.S. Secret Service's National Threat Assessment Center released a new report, Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools. As noted in the press release, the report is "the first time in agency history, NTAC specifically examines attacks that were successfully prevented. Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools examines 67 plots to conduct a school attack that were averted in the United States from 2006 to 2018." With the release of the report, USSS Director James Murray stated, "The takeaway from this report, and the 67 cases you are about to examine, is that when people come forward to report concerning behaviors, they can and do save lives…That's the bottom line, here. Bystanders save lives..."

See Something, Say Something - it applies to our places of worship, the places we go, and our schools. The report identifies a number of key findings and commonalities across the studied incidents, including:

- Targeted school violence is preventable if communities can identify warning signs and intervene.
- Schools should seek to intervene with students before their behavior warrants legal consequences.
- Students were most often motivated to plan a school attack because of a grievance with classmates.
- Students are best positioned to identify and report concerning behaviors displayed by their classmates.
- The role of parents and families in recognizing concerning behavior is critical to prevention.
- Many school attack plots were associated with certain dates, particularly in the month of April.

Read the complete report to learn more.

Spotlight: When Ransomware Strikes

Ransomware encrypts files on infected computers, making the files inaccessible until unlocked with a decryption key. Ransomware displays a warning message with a ransom demand and instructions for payment. The first documented ransomware incident occurred in 1989, but the internet has been plagued with this virulent threat since 2012.

You Are a Target. Ransomware continues impacting organizations of all types/sizes. Places of worship and other faith-based organizations are attractive ransomware targets due to valuable financial and personally identifiable information (PII) they collect. Organizations that are not prepared in advance to recover from a ransomware attack may find themselves having to negotiate an extortion payment currently over $220,000 on average to restore data, not to mention the many other financial costs and considerations involved in ransomware recovery. In addition to becoming a direct victim, faith-based organizations that outsource IT services to technology service providers (TSPs) can also become an indirect victim when the TSP is infected.

Assume Data Breach Too. Several ransomware groups are stealing and leaking data in addition to encrypting files. This has become known as "double extortion" and serves as an additional *incentive* for victims to pay a ransom even if they successfully restore systems from backup.

Get Help! If you find yourself victim of a ransomware attack, do not try to handle the incident alone! Going it alone could lead to bigger problems, including violating laws and incurring financial penalties from the government for facilitating a transaction with a prohibited entity.

Be Prepared. For more on ransomware preparedness and response, see the Ransomware Guide from CISA and the MS-ISAC.