FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Monthly Newsletter

August 2025
Volume 7, Issue 7

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level: ELEVATED

FB-ISAO Physical Threat Level for US Faith-Based Organizations: "ELEVATED."

FB-ISAO's definition of the Physical Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events. Still, there is a concern that an event is more likely than normal.

FB-ISAO Cyber Threat Level: ELEVATED

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as "ELEVATED."

FB-ISAO's definition of the Cyber Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events. Still, there is a concern that an event is more likely than normal.

Board of Advisors

Contact Us

Email

Website

How to join

Join FB-ISAO Slack Channel

FB-ISAO Events page

Mid-Year Review of Ransomware Incidents

A series of recent ransomware incidents not only highlight just how vulnerable faith-based organizations and charities are to this type of cyberattack, but these incidents also demonstrate threat actors' interest in targeting organizations that are often less prepared for a cyber incident and have a perception that they may be more willing to pay the ransom. The FB-ISAO tracks and reports on ransomware incidents affecting non-profits, faith-based and religions organizations. Our mid-year review indicates that attacks are on the rise.

Between January 01 and June 30, 2025, 36 organizations were victims of ransomware. Of those, 15 are churches, and five of those are faith-based schools.

Ransomware is a type of malicious software—or malware—that prevents you from accessing your computer files, systems, or networks and demands a ransom payment for their return. Ransomware attacks can cause significant disruptions to operations and result in the loss of critical information and data.

Below are some considerations for building ransomware resilience.

Plan. Have a cyber incident response plan (IRP) and understand that an IRP is distinct from a ransomware plan. An incident response plan, however, can encompass a ransomware response. Review the plan with your leadership, legal resource, and insurance provider.

Exercise. As with building resilience to all-hazards, hold discussion-based exercises, including executive workshops & tabletops, and also conduct drills. Consider other operational exercises.

Share Information. Information sharing builds resilience throughout communities. Assume that if your facility is a victim, then other similar facilities may be targets. After the initial emergency passes, help others within your community.

Enable Multi-factor Authentication (MFA). MFA is a way to verify user identity that is more secure than the classic username-password combination. MFA usually incorporates a password, but it also includes one or two additional authentication factors.

Patch! "Update and patch systems promptly: This includes maintaining the security of operating systems, applications, and firmware in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program." - White House Memo

Ransomware will continue to be a threat; however, building resilience is a way to minimize the impact of such incidents on an organization.

Vendor Fraud Incident

Bridgefest is an annual two-day festival held in Ocean Grove, NJ, with a 20-year history of consistent community participation and vendor engagement. Following the successful event, an incident involving suspected vendor-targeted fraud came to light. Although no disruptions were observed during the event itself, post-event reports indicate that unauthorized individuals attempted to collect payments from vendors by impersonating church representatives.

After the event concluded, organizers were informed that several vendors had been contacted by individuals claiming to represent the host church of the event. These individuals, using unofficial email addresses and aliases, offered vendor space at Bridgefest 2025 in exchange for payment. The fraudulent actors appeared to be posing as internal contacts and attempted to collect vendor fees through unverified email channels. To reduce the likelihood of similar fraud in future events, the following measures can be considered:

- ➤ Centralized Communication and Identity Verification.
- ➤ Secure Payment Procedures.
- ➤ Vendor Education and Fraud Alerts.
- ➤ Incident Response Protocol.
- ➤ Post-Event Security Review.
- ➤ Information Sharing with Peer Organizations.

Spotlight: FB-ISAO Slack! You Need to Check It Out!

Volunteers tasked with leading security programs at their houses of worship could benefit from networking with others in similar roles. FB-ISAO Slack offers such an opportunity. On FB-ISAO Slack, members share Suspicious Activity Reports (SARs), resources, and ask questions. Curious? FB-ISAO is running its annual membership sale. Join today and experience the benefits of membership for the remainder of 2025:

- ➤ Collaborate on FB-ISAO Slack
- ➤ Analytical and incident reports on security topics.
- ➤ Join live discussions and access our recording library
- ➤ Access community-centric and community-developed best practices.

Thank you for sharing this newsletter with a friend!