Pillar 9: Constant Communications

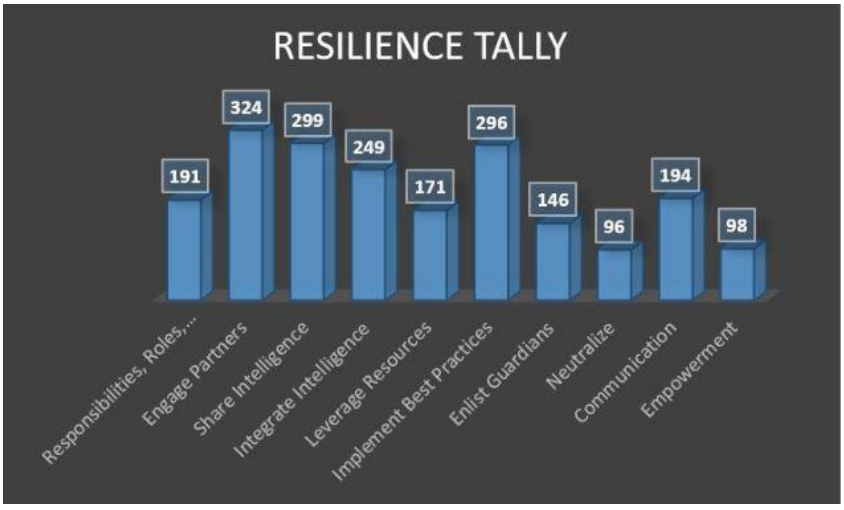
About:

Before an incident
During an incident
After an incident

All Source Approach

The ninth pillar of the R.E.S.I.L.I.E.N.C.E. model is "Constant Communications." While only mentioned a total of 194 times (as shown in the bar graph below), it is still an important pillar in making vulnerable communities better equipped for dealing with targeted violence. Houses of Worship should be in constant communication with their guardians and partners **before, during, and after** an event. This allows for better sharing of information as well as more preparedness. Communication should be done with an **all source approach**, from traditional face-to-face meetings to social media chats and posts. Any form of communication is helpful. Houses of Worship should create communication plans with their partners immediately.

While both pillars are similar, there is a difference between "Constant Communications" and "Sharing Information and Intelligence." The third pillar of the model emphasizes the need to spread spiritual awareness about potential threats. It is more focused on preventing incidents through the sharing of knowledge. While this is incredibly important in avoiding attacks and learning more about the community, the ninth pillar goes more into depth about how to better work with partners and guardians during an event as well as after. Steps should be made to ensure "Constant Communications" with all stakeholders to be better prepared in the event of an attack.



Importance:

"Constant Communication" is vital in preparing the community for an incident, as well as assigning roles during/after an attack and sharing information and intelligence (Pillar 3). Before an incident can occur, communication allows for the exchange of knowledge about any potential threats or preventative measures. Houses of Worship can use this knowledge to become better educated about the evolving threat paradigm and how to best protect their communities. During

an event, "Constant Communications" allow all stakeholders to know exactly what is going on and what they can do to stop the perpetrator or help any victims. People can explain where they are for help to arrive, as well as where the attacker might be located. Communication would help allow an incident to be halted immediately. After an attack, Pillar 9 allows all members to communicate with each other to step up the security, provide any services to victims, and figure out the next steps. Pillar 9 can aid in the healing process and get the community back on their feet.

Without communication, plans can quickly fall apart. People become unaware of what roles they should be carrying out. Steps can be overlooked and members may focus on matters unrelated to the situation at hand. Imagine working on a group project, but no one is talking to each other or saying which parts they are doing. The same thing applies– during or after an incident of targeted violence, without communication, all stakeholders would be left confused as to what they should or should not be doing. "Constant Communication" is vital in properly working together in a unified fashion.

As shown in the diagram above, "Constant Communication" is very important in building resilience in Houses of Worship. It is not its own separate portion of the wheel, rather, it is an aspect of R.E.S.I.L.I.E.N.C.E. that is carried throughout the rest of the nine pillars. It is important to properly communicate any crisis plans and ensure that every stakeholder understands what is going on, whether through engaging partners (Pillar 2) or implementing best practices (Pillar 6).

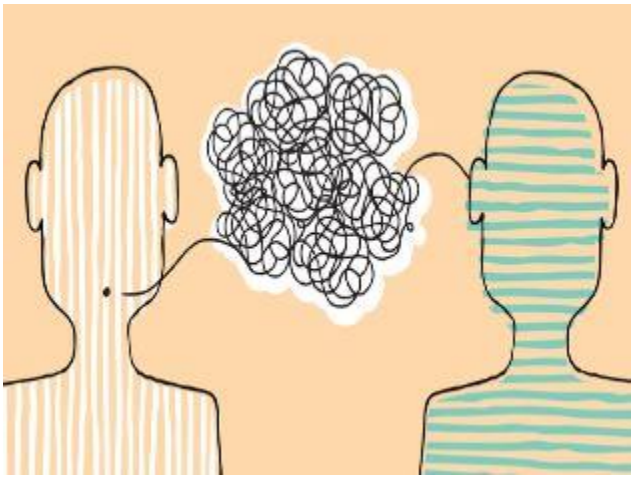
To recap, Pillar 9 is important for the following reasons:

1. Sharing information before an incident for preventative measures.
2. Sharing information during an incident to quickly get help and stop the attacker.
3. Creating more organized crisis plans and assigning roles.
4. Healing the community together after an incident.

"Somebody will be assigned to speak to the media, somebody assigned to make sure that every member of the congregation or organization is contacted if something happens and is instructed on how to react and what to do."
- John Farmer

Internal vs. External Communications

There are two types of communications when working in teams before, during, and after an incident of targeted violence. There is the Internal Communications and the External Communications. These types are separated according to how closely the individuals are impacted by the attack. Those who are most affected would most likely be within the congregation in a House of Worship, while those who are not as affected would be external to the faith group.



Internal Communications consists of communication among those immediately impacted by an attack. This includes any faith leadership, security and safety teams, and the faith community. All forms of communication occur within the House of Worship and their members. This can be done through face-to-face gatherings, social media chat groups, or even religious events.

External Communication occurs between those impacted and the external, local community that responds to an incident. This includes first responders and the media. This type of communication can also consist of face-to-face gatherings or social media, but on a less personal level.

Recommendations:

Communicate, communicate, communicate. The key in building resilience in Houses of Worship is to *talk* to all partners and guardians, whether through talking face-to-face or through social media technologies. By communicating, vulnerable communities can become more prepared and trust is built.

"I mean, this business of emergency response is all about relationships and being able to communicate, first and foremost…"
-Kona Zoganas

Develop a Communications Plan

Create a *Steady State Communications Plan* that allows all stakeholders to communicate with each other on a regular basis. This is when things are going smoothly and "steady." This kind of plan can consist of weekly or biweekly phone calls or outings, frequent emails, or social media chat messages. One idea can be a Facebook group that allows all members to freely communicate with each other about various topics, safety plans, and more.

A *Crisis Communications Plan* should also be implemented so that in the case of a crisis, such as targeted violence or mass casualty attack, all stakeholders will know how to contact each other and call for help. Plans can include hotlines, the number for first responders, roles and responsibilities for each member (such as getting people to safety and speaking to the media), as well as areas to regroup during or after the incident. There can also be a group-chat with all stakeholders reserved for crisis situations to further communicate and assign roles. Attacks will not go according to plan and improvisation will be needed, so communication is vital in becoming flexible to the threat.

Communicate Threats through Programs

Implement programs that allow all members of the community to communicate threats. This can include the SAR program, S4, as well as tech/apps/smartphones. Houses of Worship can use available programs as guidelines to create their own initiatives to communicate with their partners and other faith leaders.

See Something, Say Something

The *SAR program*, or Suspicious Activity Reporting, is part of the Nationwide SAR Initiative, or NSI, which is run by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and law enforcement. It allows for the sharing of any suspicious activity as well as a means to gather this information, document it, process, and analyze it. This program helps law enforcement to get a better sense of the present threats and create ways to prevent terrorism. Houses of Worship can use the SAR program to better understand how members of their community can report on suspicious activity.

S4 is well known and said everywhere to everyone: *see something say something*. All members of the community should remember to keep an eye out on their surroundings. If they see anything suspicious, they should report it to their faith leader or communicate with their local law enforcement.

"Be a part of your communities. Step out. Teach your kids. We're all in this together and when we're all in this together, you have a resilient community … you have to build that trust and demonstrate you're trustworthy as well as reaching out to others"

-Russ Deyo

Vulnerable communities can also implement their own programs using evolving technology. Cellphones and laptops allow members to easily connect with each other and share information via text messaging or emails. There are also many apps and social media platforms that can permit all

stakeholders to communicate or share information about suspicious activity. Houses of Worship should take advantage of the available technology and communication platforms and apps to create programs that communicate threats.

Establish Communication Partnerships, Plans, and Organizations

Information Sharing and Analysis Organizations help vulnerable communities by "identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices." Created by the U.S. Department of Homeland Security, members of ISAO work with all stakeholders to create best practices and implement information sharing. Houses of Worship should establish partnerships with organizations such as ISAO to better understand how to communicate with all members of the community and gain knowledge of best practices.

Information Sharing and Analysis Centers are similar to ISAO's in that they strive to communicate all threats and mitigation information to their clients. These centers help in collecting, analyzing, and disseminating all available threats. They would then share this information with their partnerships. In addition to ISAO, Houses of Worship should establish a communication partnership with ISAC to learn of all available threats and how to mitigate them with tools that ISAC provides.

The *National Interagency Coordination Center* coordinates where resources go throughout the United States in response to events such as wildfires or any other incident. NICC can help vulnerable communities by providing the tools they need to respond to targeted violence or create preventative measures. It is highly recommended that Houses of Worship create a communication partnership with NICC to ensure the necessary resources before and during an incident.

The *National Cybersecurity and Communications Integration Center* was established by DHS to "reduce the risk of systemic cybersecurity and communications challenges" and is the "national hub for cyber and communications information, technical expertise, and operational integration." NCCIC also educates the public on risks and how to best mitigate them. This center would be a very resourceful partnership with Houses of Worship.

Local *FBI Field Offices* would also be important communications partners to have. Not only would they be able to provide vital information about any existing threats local to the vulnerable communities, but they could also provide the resources needed to combat any targeted violence. A close relationship with the local FBI would build trust and resilience within the community.

Fusion Centers are central points where intelligence from every agency and organization is shared and exchanged. Houses of Worship are highly recommended to create communication partnerships with these centers in order to stay updated on any threats.

Leverage Technology

As mentioned briefly before, vulnerable communities should leverage technology to their advantage. Violent extremists are using it to communicate and mobilize with each other, and vulnerable communities should do the same. Technology is always evolving to become faster and more reliable, making devices such as smartphones become the best way of communication. All stakeholders should use instant messaging, emails, social media, and other apps to communicate with everyone involved. Technology allows for a multitude of ways of communication: texting, video chatting, calling, and emailing. Use these resources for "Constant Communications" and become a more resilient community.

Build Redundancy within the Community

Redundancy is defined as information that is expressed numerous amounts of times. While the information can be repetitive – communicate, communicate, communicate – it is important that all stakeholders are aware of the resources available to them and how to best contact each other. They must stay on top of the evolving threats and technologies, and the plans of communication. You should build redundancy within vulnerable communities so that in times of crisis, they will remember what to do and who to contact.

"Even though we tell them it doesn't replace 911, but we want to build redundancy in the event you get into a stressful situation. Sometimes even dialing 911 could cause you to fumble on your phone. So we simplified it with technology. These panic alarms go directly to the police emergency radios… so we've built in a backup to the back up and we test that all the time. One of the things we want to make sure is that everyone's familiar with it."

-Jim Hartnett

Sources

https://nsi.ncirc.gov/

https://www.isao.org/about/

https://www.nationalisacs.org/

https://www.nifc.gov/nicc/

https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center