RUTGERS
UNIVERSITY | NEW BRUNSWICK

Eagleton Institute OF Politics

Building the Resilience of Citizens, Communities, and Countries
A Rutgers Longitudinal Study of Principle-Based Policies and Practices
Chapter One: Houses of Worship and Vulnerable Communities

Dr. Ronald J. Clark

> *Terrorism and mass violence cannot prevail if people refuse to be terrorized. If people are resilient, if they return to their houses of worship, the assailant fails...*
>
> *- Jeh Johnson, Former Secretary of the U.S. Department of Homeland Security*

TABLE OF CONTENTS

Building the Resilience of Citizens, Communities, and Countries

A Rutgers Longitudinal Study of Principle-Based Policies and Practices

Chapter One: Houses of Worship and Vulnerable Communities

INTRODUCTION

The study on Building the Resilience of Citizens, Communities, and Countries research is a Longitudinal Study of Principle-Based Policies and Practices across multiple sectors, domains, and populations. The chairman of the study and author is Dr. Ronald Clark, the former Deputy Under Secretary at the U.S. Department of Homeland Security. The intent of the longitudinal study is to identify and validate principles that build the resilience of citizens, communities, and countries.

Each chapter of the study explores a range of proven principles, practices, protocols, and plans. The first chapter of the study—embodied in this report—focuses on houses of worship and the vulnerable communities they serve. Subsequent chapters of the study will examine other sectors, communities, and will ultimately explore national resilience. Every section integrates multiple sources of evidence including voices of experience captured in formal qualitative interviews, case studies, and a review of the literature. This evidence-based approach is designed to elicit principles and practices that serve as guideposts to counter current and emerging threats and challenges. The research is further informed by the enduring work of the Eagleton Institute of Politics with vulnerable communities in the United States and Europe, and dozens of interviews with Cabinet-level ministers, experts, first responders, and affected community members.

Finally, the research and evidence base assess the efficacy of the author's principle-based RESILIENCE Model for houses of worship and vulnerable communities. A model created while serving at the National Security Council and the Department of Homeland Security. The resilience framework is explained, explored, and applied in the coming sections. It ultimately serves as the structural framework and guide for this study.

Three Research Challenges – Ecosystem, Evidence, and Applicability

In the first chapter, "Houses of Worship," the research team faced three core research challenges: the need to address the reality of a broader ecosystem; the need to identify evidence-based principles to inform best practices; and the imperative that the framework enjoy broad and enduring applicability.

To address these challenges, the author created a strategic study framework that builds the ecosystem across a series of seven chapters and launched an evidence-based best practices study. The first research chapter as indicated focuses on houses of worship serving vulnerable communities, within small communities or large cities. From this initial chapter, the study will build across domains and sectors, culminating in evidence-based principles and practices for national resilience in future reports.

Ecosystem Challenge

The fundamental reality is that in the United States alone there are over 350,000 houses of worship that all exist within a broader ecosystem of communities. Houses of worship are interconnected with the broader citizenry and community. To effectively secure and protect houses of worship, one must assess, plan, and act within this strategic context. As Andy Jabbour noted eloquently in his interview, houses of worship cannot be islands unto themselves. Crime and terrorism, be they in the physical world or cyber domain, know no boundaries. A community rife with internal strife, crime, or terrorism, whether it be domestic or foreign, ripples across all sectors, all businesses, and all houses of worship. Any effort to assess and prepare a house of worship must be taken within this interconnected context.

> *Threats aren't isolated typically to one house of worship or one faith or one type of organization. A house of worship can't be an island of its own, and just pray for safety and security and trust God to take care of them; they have a responsibility to be an active participant in their own well-being.*
>
> *- Andy Jabbour, Cofounder, Faith-Based Information Sharing & Analysis Organization (FB-ISAO)*

This seemingly obvious reality created a fundamental challenge for this research project. Where to start? How could the study avoid the perils that have impacted other efforts? How could the author boil the ocean in a way that avoids the obvious downside of researching, assessing, and developing best practices that are myopically focused on a subset of infrastructure in the United States and across the globe? The faith-based context is unquestionably important, but is admittedly a sub-set of a much larger sector that nests within sixteen critical infrastructure sectors. These sixteen sectors range from government facilities to financial institutions to commercial facilities. Fundamentally, there are two competing challenges: the need to look at houses of worship within the right strategic context and the requirement to discover evidence-based best practices that are specific and useful to communities of faith. The multiple chapter structure is intended to address this challenge. The first chapter explores communities of faith, and subsequent chapters will expand from this starting point.

Evidence-Based Challenge

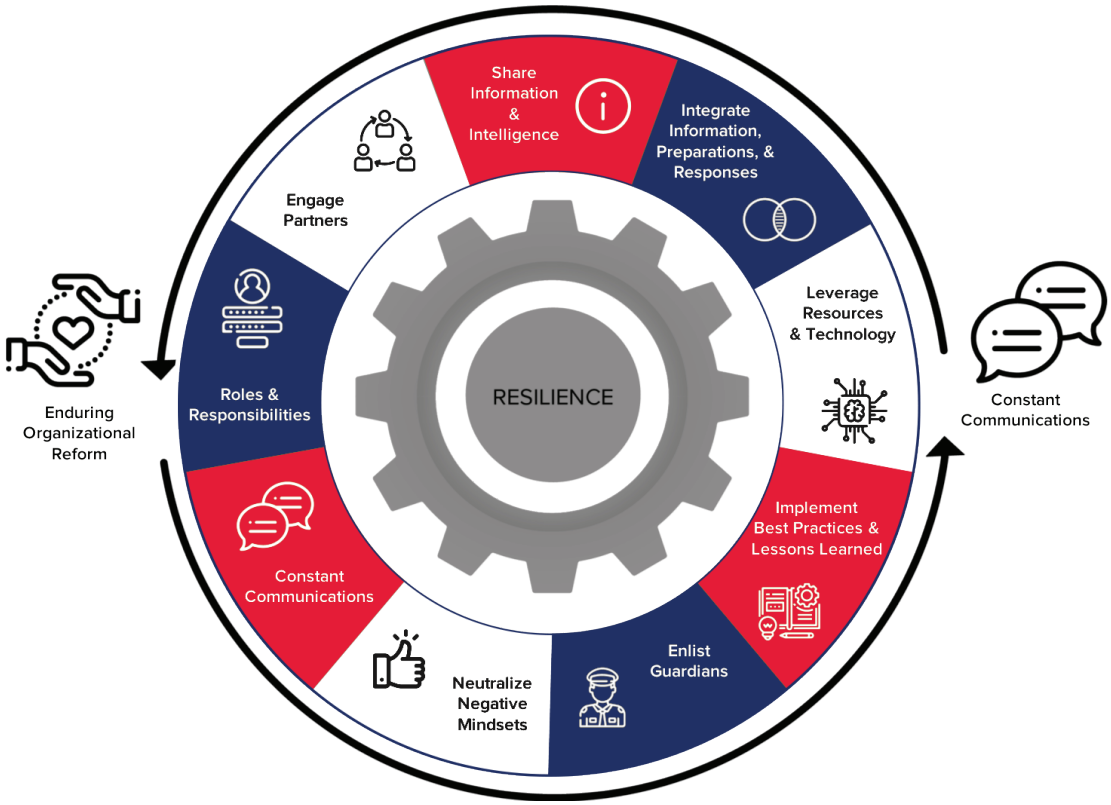
The assessment from Rutgers University subject matter experts was, universally, that there was a distinct need for evidence-based best practices for houses of worship. Not best practices born from the keyboard of a well-intended writer, but practices rooted in evidence. This evidence should be derived from a broad and significant community of experts and practitioners. To this end, the author launched a longitudinal qualitative study that would integrate interviews with a broad community of leaders, experts, and practitioners. The interviews would be reinforced by case studies and grounded in a literature review.

Applicability Challenge

The next challenge the author faced was how to make this universally applicable to 350,000 houses of worship. How can a study be made applicable to both a large urban mosque and a small rural church? The answer was rooted in the need to conduct research that would create an evidence base that would guide the team to enduring principles – an evidence base that would lead us to those practices that possessed the greatest veracity. The path was to find, discover, and validate enduring principles. To identify and determine if the author's RESILIENCE Model had efficacy for houses of worship. The journey to evidence-based best practices was the path taken to ensure that this effort would be relevant and viable for the broadest possible set of communities.

Brief Study Overview

The chosen methodology for the study is qualitative. The study employed an emergent design for the collection of data through open-ended interviews. All of the 31 semi-structured interviews were formally recorded. Once recorded, the interviews were transcribed and then coded using the ten principles of the RESILIENCE Model. The study used the procedures of peer debriefing, member checking, thick description, and a complete audit trail. These procedures were designed to establish credibility, transferability, dependability, confirmability, and the ultimate trustworthiness of the study. With the establishment of trustworthiness, readers may then move to conclusions that are well reasoned, informed, and potentially transferable.



THE RESILIENCE MODEL

While serving on the National Security Council and later as a Deputy Under Secretary at the Department of Homeland Security (DHS), the author developed what was internally called the Clark Resilience Model (CRM). The CRM was the product of three sets of service and experiences for the author: decades in the Marine Corps operating overseas as an infantry officer, a half-decade at the National Security Council, and finally, service as a Deputy Under Secretary at DHS. The CRM served as an internal guide that the author revised over time as new experiences and evidence emerged. The CRM helped guide strategic deliberations on resilience as the author's team of 16,000 law enforcement, Federal, and contracted team members worked tirelessly to secure the vast infrastructure of the United States. The focus was to, over time, as experience and evidence mounted, identify, test, and integrate potential principles. Principles grounded in evidence. Principles that would represent a broad and sustained distillation of enduring knowledge. Knowledge that would be broadly applicable and equally relevant to a large house of worship in an urban area or small community center in a rural area.

The model proved relevant and sound within the context of service in the Department of Homeland Security and the White House. However, a core question for the study was: will the qualitative evidence validate and correlate with the principles of the CRM? Or would the CRM be something that was contextually bound as a senior leader guide that was less relevant for houses of worship? The bottom line up front is that the qualitative evidence base derived from this study, which consisted of 31 coded formal interviews and evidence gleaned from more than 130 conferences, seminars, and informal interviews, overwhelmingly validated the RESILIENCE Model. This produced thousands of validating connections with the RESILIENCE Model and, most important, a rich repository of evidence-based best practices. The following sections of the report and guide will translate and apply these evidence-based best practices.

The R.E.S.I.L.I.E.N.C.E. Model Principles

In the early days of thinking through a RESILIENCE Model, the author created more complex systems that took longer to communicate, understand, and retain. To enable rapid communications and facilitate retention, the author developed the principles of the CRM. Once the principles were in position, he next worked on crafting them into an acronym. The acronym became R.E.S.I.L.I.E.N.C.E. and the intent was to make it easy to communicate, remember, and act upon.

1. Roles and Responsibilities
2. Engage Partners
3. Share Information and Intelligence
4. Integrate Information, Preparations, and Responses
5. Leverage Resources and Technology
6. Implement Best Practices and Lessons Learned
7. Enlist Guardians and Execute the Plan
8. Neutralize Negative Mindsets
9. Constant Communications
10. Enduring Organizational Reform

The **R.E.S.I.L.I.E.N.C.E.** Model is grounded in ten principles:

Roles

The first principle of the R.E.S.I.L.I.E.N.C.E. Model is "Roles and Responsibilities." To ensure the resilience of houses of worship, critical roles need to be identified and responsibilities assigned. The first step is to get organized and align the right people with the right roles and responsibilities. Think of it as who's doing what, to whom, when, and why?

Engaging

The second principle of the R.E.S.I.L.I.E.N.C.E. Model is "Engage Partners." Its focus is on creating relationships with fellow citizens, congregations, and communities. It is about engaging all members, including local partners, state stakeholders, and Federal organizations. By "Engaging Partners," houses of worship build trust and relationships. The resulting connections unify individuals, institutions, and communities against common threats – be it crime or perpetrators of violent extremism.

Sharing

The third principle of the R.E.S.I.L.I.E.N.C.E. Model is "Share Information and Intelligence." The goal of this principle is to gather, analyze, and share information and intelligence with partners at the community, city, and national level (as applicable). The intent is to enhance the situational awareness of vulnerable communities and houses of worship. Gathering and sharing information builds connections, contacts, and mutual trust. (Note: houses of worship will traditionally be involved with the exchange of information rather than actual intelligence documents.)

Integrating

The fourth principle of the R.E.S.I.L.I.E.N.C.E. Model is "Integrate Information, Preparations, and Responses." The centrality of this pillar is at the core of the RESILIENCE Model. The fourth principle is a key gear that leverages the efforts and impact of the other principles and becomes a key driver for the institutionalizing of a culture of security. It is also one of the broadest principles, covering plans, training, exercises, and crisis response.

Leveraging

The fifth principle of the R.E.S.I.L.I.E.N.C.E. Model is "Leverage Resources and Technology." To prepare well there is a distinct need to assess and enlarge current and future resource pools. The key is to know your resources and to seek additional support through public and private organizations. Developing access to resources can enable the procurement of low-cost, high-impact technologies that can reinforce security measures.

Implementing

The sixth principle of the R.E.S.I.L.I.E.N.C.E. Model is "Implement Best Practices and Lessons Learned." Implementing best practices and lessons learned can significantly reduce the threat to vulnerable communities and houses of worship. Lessons learned can be derived from direct or indirect experiences. Indirect experiences offer houses of worship the opportunity to leverage and integrate lessons learned from other institutions. The key is that a lesson is only learned once implemented!

Enlisting

The seventh principle of the R.E.S.I.L.I.E.N.C.E. Model is "Enlist Guardians and Execute the Plan." The focus of this principle is to mobilize guardians and execute. These can range from volunteer ushers who welcome people into the facility to full-time security staff. The difference between this principle and the second principle, "Engage Partners," is that it focuses on the direct recruitment, development, and deployment of guardians for the direct defense of the house of worship vice the creation of a broad network of relationships. The forming of pre-crisis relationships in the second principle is a critical step for enlisting guardians.

Neutralizing

The eighth principle of the R.E.S.I.L.I.E.N.C.E. Model is "Neutralize Negative Mindsets." The focus of this principle is to ensure an empowering philosophical and psychological paradigm and to reject negative mindsets. Negative mindsets are driven by false premises like "this will never happen to us," "what can we do about an active threat," or "this is inevitable." Negative mindsets degrade preparations and ultimately, responses. They curtail a security culture from taking root. The right empowered mindset is the product of input and collaboration with a variety of internal and external stakeholders.

Communicating

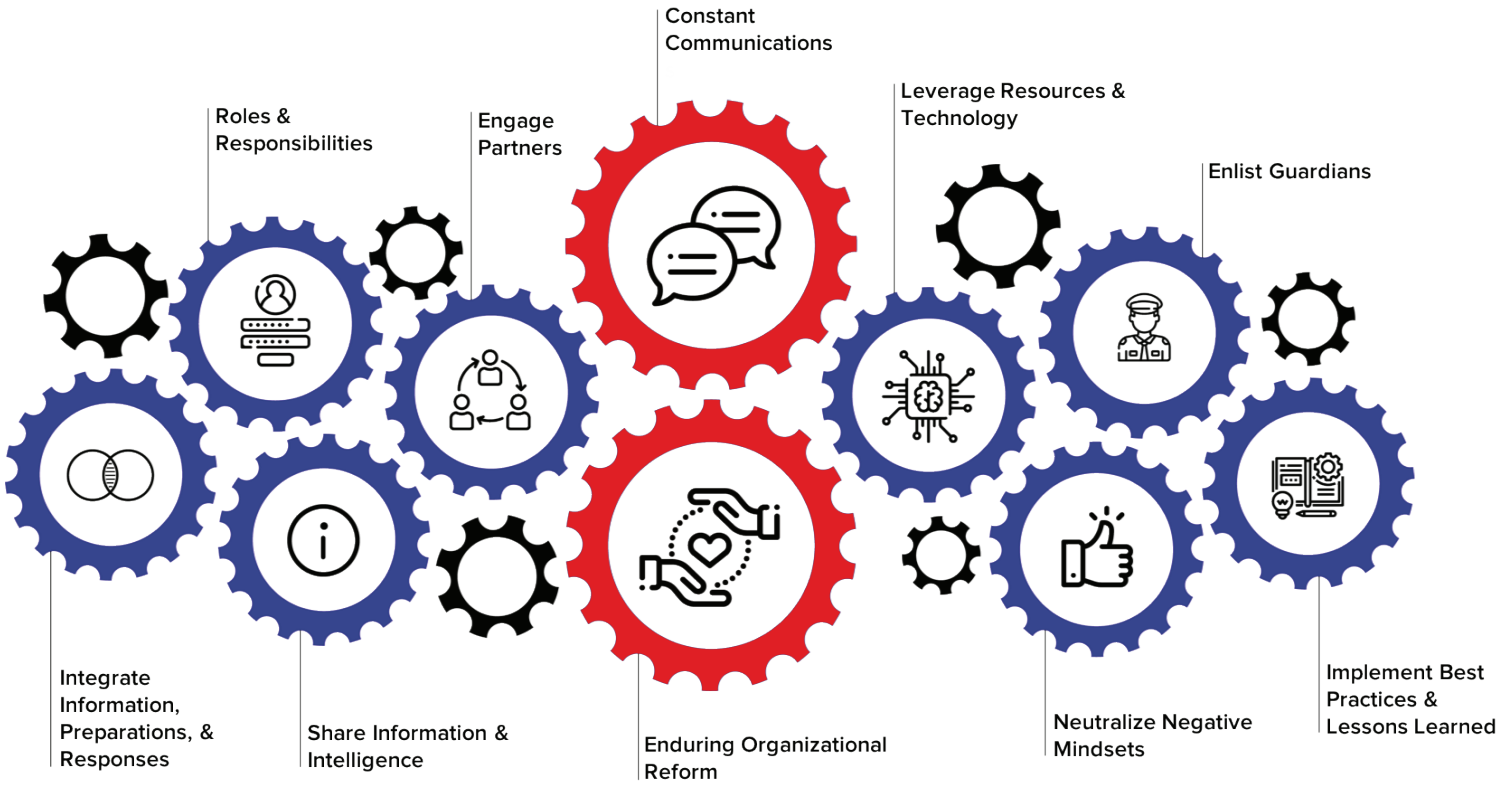
The ninth principle of the R.E.S.I.L.I.E.N.C.E. Model is "Constant Communications." Houses of worship must be in constant communication with their congregation, partners, and guardians. All of this must start before a crisis and must continue through the event and into recovery. Communications must be done with an all source and method approach.

Enduring

The tenth principle of the R.E.S.I.L.I.E.N.C.E. Model is "Enduring Organizational Reforms and Readiness." The final principle of the model is focused on the need to codify and institutionalize safety and security practices to ensure lasting reforms and readiness. This is a long game against an unpredictable set of adversaries with different motives, tools, tactics, and procedures. Houses of worship must prepare today and sustain those preparations into perpetuity.

A Systems Approach

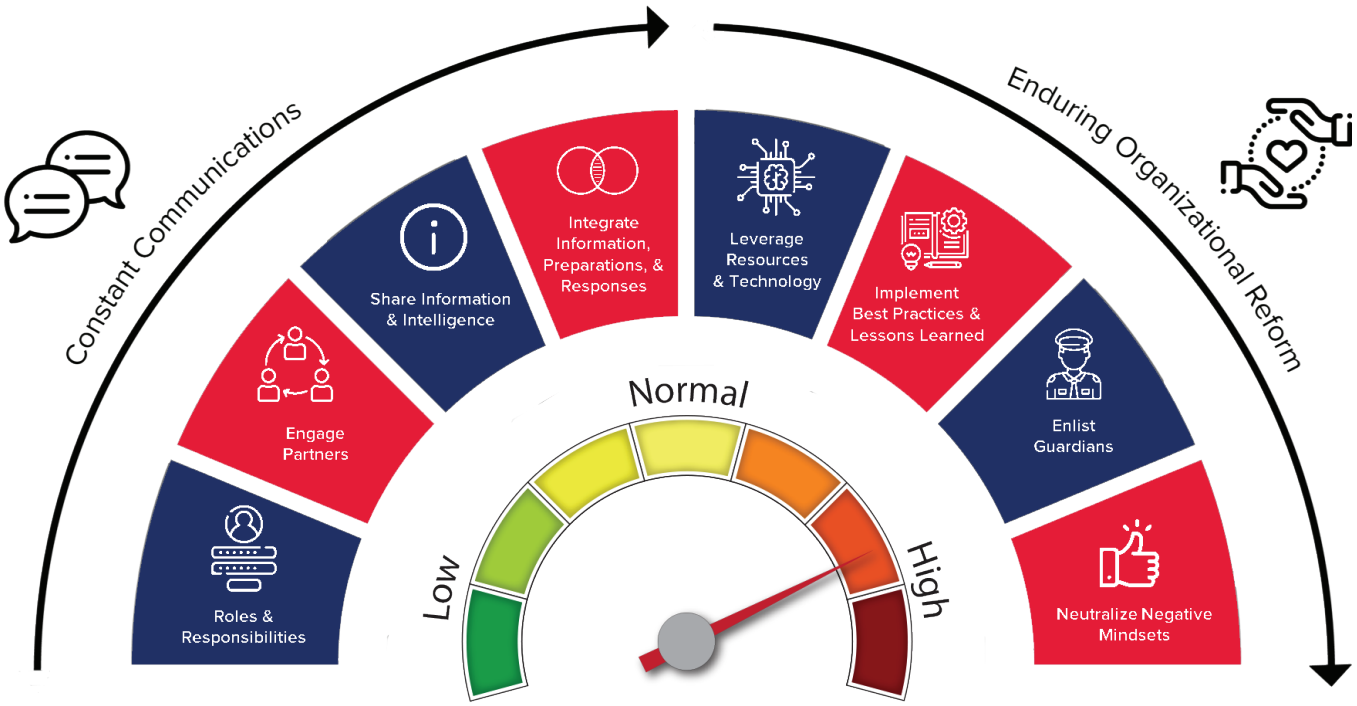
The RESILIENCE Model offers an evidence-based system. It is grounded in principles that serve as enduring best practices and guideposts. These principles are integrated into a system that provides a structure or an architecture that enables a systematic and holistic approach. The employment of a holistic approach is also a validated best practice. The model offers a multi-dimensional solution to a complex and evolving range of threats. Threats that include physical and cyber attacks. Challenges that range from preparing for and recovering from natural disasters to active threat events.



An Interconnected System of Systems

The ten principles of the RESILIENCE Model are interdependent and together produce a synergistic effect. The model's principles work like the gears in a machine or a clock. Each principle is individually important and essential to the ultimate efficacy of the model. However, together they produce an outsized impact on measures designed to protect, prevent, respond, and recover from the full range of events. For example, the "Engaging Partners" principle directly supports and is supported by principle three, "Share Information and Intelligence." Actively reaching out to internal and external, public and private partners creates the human network vital for the sharing of information and intelligence.

1. **R**oles & Responsibilities
2. **E**ngage Partners
3. **S**hare Information & Intelligence
4. **I**ntegrate Information, Preparations, & Responses
5. **L**everage Resources & Technology
6. **I**mplement Best Practices & Lessons Learned
7. **E**nlist Guardians & Execute the Plan
8. **N**eutralize Negative Mindsets
9. **C**onstant Communications
10. **E**nduring Organizational Reform



RESILIENCE Model as Assessment Tool

From Assessment to Action

The RESILIENCE Model provides an assessment that is postured for action. Once assessed along ten principles or lines of effort, the assessment phase is naturally mapped to action. This crucial transition from assessing to acting is vital. All too often, institutional assessments of resilience stop at the review process. A very expensive and time-consuming effort to review every aspect of security, plans, roles, and actions turns into a robust report that sits on someone's desk. The sheer complexity and volume can become a barrier to entry. In contrast, the RESILIENCE Model is a system designed to reduce friction and enable action. Whatever assessment method is selected ensures that it serves as an action-forcing mechanism!

Assessment as a Cycle

The other key point is that the assessment process is not a static, one-time event. Each assessment is only a snapshot in time, based on current security protocols and threats. As institutions evolve and new threats emerge, security protocols may need to change. Assessing periodically with a set model or methodology also affords the ability to track progress or regression. For example, a house of worship with a long-time director of security who moves to a new city or retires could find their resilience impacted by this transition. It could result in a critical gap in the capacity of the institution to engage partners, share information, and effectively maintain clear roles and responsibilities.

THREAT ENVIRONMENT

The current threat environment is increasingly unstable and unpredictable. It is replete with an expanding range of globally connected actors intent on inspiring, enabling, directing, or delivering increasingly disruptive attacks against communities of faith. Absent a direct and sustained intervention effort, attacks against houses of worship will likely proliferate in scale, impact, and tragic frequency.

> *We have to always stay one step ahead of the threat picture. We can't just respond to the last attack; we have to anticipate the next one.*
>
> *- Jeh Johnson, Former Secretary of the U.S. Department of Homeland Security*

According to the Federal Bureau of Investigation (FBI), DHS, and other fusion center sources, houses of worship and other faith-based facilities will continue to be potential targets for terrorists and homegrown violent extremists (HVEs). Enhanced communication, coordination, and training among Federal entities, state, local, tribal, and territorial first responder agencies, religious community groups, and private sector partners can improve security protocols, increase awareness of suspicious activity indicators, and ultimately improve the ability to detect, deter, and disrupt potential plots.

Notably, the study revealed a series of profound insights into the threats against houses of worship and, more broadly, vulnerable communities. In the interest of time, let's review three of these findings.

Enduring Awareness Challenge

All of the 31 formal interview participants identified a systemic lack of threat awareness. The unanimous assessment was that awareness of tactical and local threats was severely lacking across the communities. An understanding of how geostrategic events impact communities was virtually absent. Although pockets of awareness were of course recognized, the vast majority of citizens and local communities lacked a fundamental understanding of the threat. Furthermore, the assessment from those formally interviewed indicates that there is a profound lack of institutional mechanisms to receive and report threat information.

Physical Threats Universally Recognized

Universally, the 31 formal interview participants identified significant physical threats to houses of worship, ranging from ideologically-inspired active shooter attacks to criminal operations. The formal interview participants also recognized the disruptive to destructive impact of natural disasters. Some reflected upon their experiences in New Orleans following the catastrophic effects of Hurricane Katrina on the city and on houses of worship.

Cyber Threats Universally Unrecognized

In stark contrast to the universal recognition of the physical threats to houses of worship, the majority of interview participants did not address cybersecurity risks. One notable exception was the CEO of a cybersecurity company. He not only highlighted the issue, but also assessed the cyber threat to houses of worship as significant. This threat is clearly compounded by a profound lack of awareness, an expanding attack surface as vulnerable communities become increasingly connected, and by significant cyber defense capability shortfalls.

> *There's zero awareness! People have no idea regarding their significant cyber risks. And worse, people just automatically assume, well, that only happens to big companies. That doesn't happen to us. You know, nobody would care about us. I hear that all the time. Clients have been breached? Well, nobody would care about us.*
>
> *– Brian Dykstra, CEO*
> *Atlantic Data Forensics*

All Sacred Houses, All People, All Places, All the Time

The bottom line from the formal interviews and over 130 informal sessions is that a persistent and increasingly capable set of adversaries threatens all sacred houses, all people, all places, all the time. A terrorist-inspired homeland attack on faith-based organizations could include the following tactics:

Active Shooter. Active shooter scenarios may include proximity-based incidents in which the attacker is near the intended victims, but may also include situations where crowds are targeted from afar using large caliber rifles or other weapons.

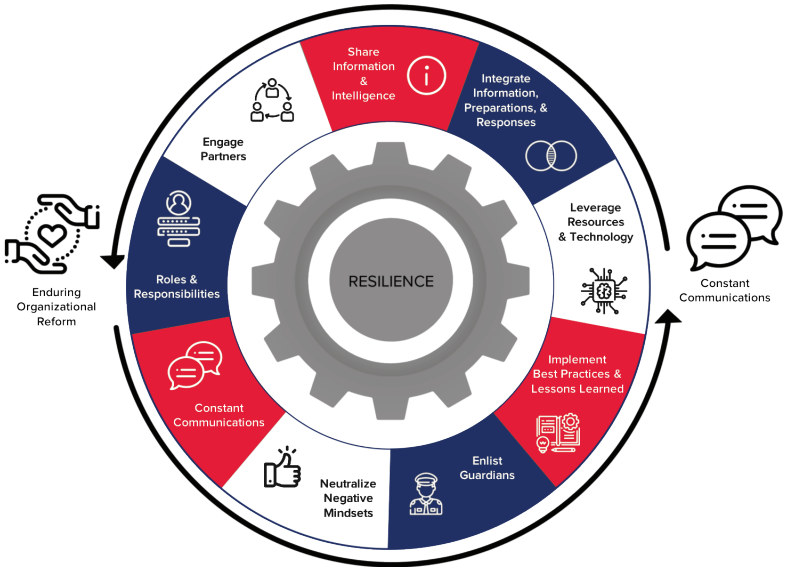
Explosives or Incendiary Devices. Explosive attacks include a variety of devices and delivery methods. These include Improvised Explosive Devices (IEDs) placed in backpacks, vests, or vehicles. The complexity and potency of an explosive device are highly variable and depend on the expertise of the bomb maker and their access to explosives or homemade explosive precursor materials. A recent international attack on multiple houses of worship used backpack IEDs that produced hundreds of casualties in a matter of seconds.

Arson. In the absence of access to industrially produced or improvised explosives, arson is a disruptive and potentially destructive tactic that can be executed using readily available materials. A string of recent attacks in the southern United States used arson with telling effect. In some cases, it resulted in the significant destruction of the targeted building.

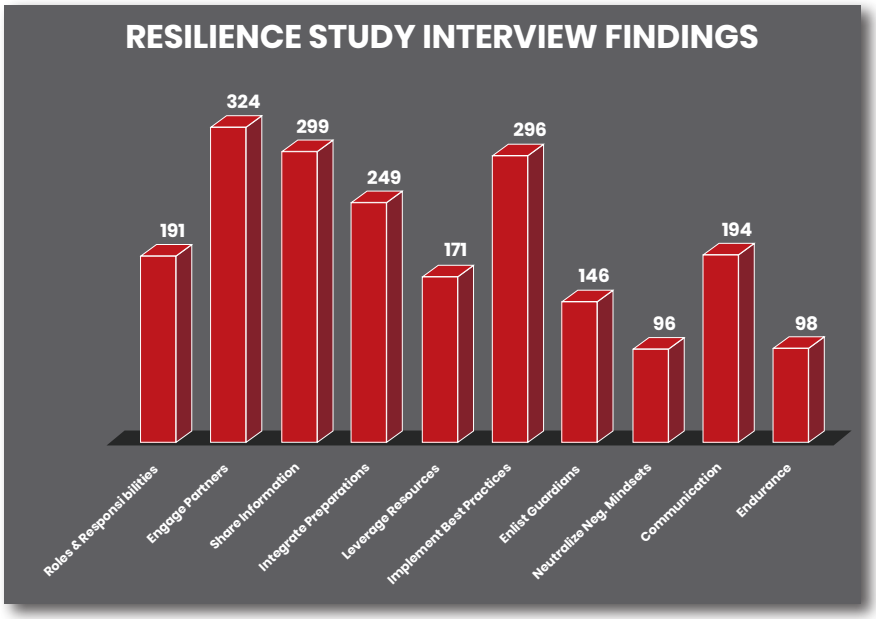
Vehicle Ramming. Terrorists with limited access to explosives or firearms may attempt to leverage the use of motor vehicles – to include commercial trucks – as ramming weapons, offering an opportunity to conduct an attack that requires only minimal prior training or experience.

Edged Weapons. These attacks require only minimal preoperational planning, as the weapons are easily accessible and can be used to support other tactics.

Cyber Weapons. The volume, variety, and velocity of cyber attacks are increasing at alarming rates. These attacks can result in the exploitation of personally identifiable information, to the defacing of websites and the theft of financial resources.



PRINCIPLE 1: ROLES AND RESPONSIBILITIES



The first principle of the RESILIENCE Model is "Roles and Responsibilities." To ensure the resilience of houses of worship, the identification of key security roles and the assigning of responsibilities is essential. The first step is to get organized and align the right people with the right roles and responsibilities. Think of it as "who is doing what, to whom, when, and under what conditions." It is a principle well validated within this body of research. The principle of "Roles and Responsibilities" within the RESILIENCE Model was discussed in formal interviews more than 190 times by the vast majority of research participants.

Internal and External Stakeholders

Heads of congregations or religious leaders have a broad family of internal and external stakeholders that should be mapped and engaged. This natural team of stakeholders provides a range of options for organizing an institution's security to communications roles.

Internal Stakeholders

For any house of worship, there are seven critical roles executed by an internal team as small as two or as large as seven people. These roles are outlined on the next page. These sizing constructs are dependent upon the density of qualified staff, volunteers, and the size of the institution.

External Stakeholders

The internal team will then be reinforced by external stakeholders. External stakeholders include local, state, and Federal law enforcement, fire, and emergency medical personnel. Their role is to ensure the coordination and execution of their primary professional responsibilities for a house of worship. This is done in close coordination with those who know the house of worship best.

Organization of Roles

There are seven key roles, with associated responsibilities, that can be supported by an individual director for each one or consolidated into just two people. If the seven roles and responsibilities are consolidated into two people, one would serve as the Chief Security Officer and the other as the Chief Communications Officer. The Chief Security Officer would be responsible for the following roles: Director of Security, Director of Cybersecurity, Director of Information, and Director of Plans, Policies, and Training. The Chief Communications Officer would be responsible for the following roles: Director of Communications, Director of Resource Management, and Director of Administration. Basically, the Chief Security Officer handles all the physical and cyber preparations and responses, while the Chief Communications Officer is responsible for all internal and external communications, resource management, and administration.

Two Key Officers

- **Chief Security Officer (CSO)**
  - Roles: Security, Cybersecurity, Information, and Plans
- **Chief Communications Officer (CCO)**
  - Roles: Communications, Resource Management, and Administration

The Board of Seven (Alternative Structure)

- **Director of Security**
  - Responsible for all aspects of safety and physical security preparations and responses.
- **Director of Cybersecurity**
  - Responsible for all aspects of cybersecurity preparations and responses.
- **Director of Communications**
  - Responsible for all communications in steady state and in crisis.
- **Director of Information**
  - Responsible for the sharing, receiving, processing, and integrating of all information.
- **Director of Plans, Policies, and Training**
  - Responsible for all assessments, plans, training, and exercises.

- **Director of Resource Management**
  - Responsible for all security and safety-related resource management from external grants to internal funding.
- **Director of Administration**
  - Responsible for all aspects of safety and security administration.

Key Teams

Every role and its corresponding director or chief are supported by a team. The teams consist of internal and external stakeholders. The internal team for a house of worship will likely consist of professional staff and volunteers. These internal teams will work closely with first responders, other members of the community, and other houses of worship. These teams will change over time and as situations dictate. For example, in support of services on a special day, the standing security team will likely be augmented with additional volunteers.

Key Committees

Any number of committee structures are viable for a house of worship. Some committees will be permanent, while others are constituted as needed. For example, an assessment committee might be constituted for an annual or bi-annual review, while the standing planning committee is in effect year-round. In contrast, the crisis response committee would also be a standing committee, but it would only be constituted in emergencies. In general, a committee for crisis or emergency management, steady state operations, and planning are important structures to have in place. Most notably, the crisis action team would consist of all seven directors or the two chiefs, the head of the congregation, and external stakeholders such as a designated first responder liaison.

> *You must establish internally a committee of people to handle emergencies, and then establish liaisons with both police and other faith communities so that they know the point people in crisis, and who is empowered to speak on behalf of a faith community if under attack.*
>
> *- John Farmer, Former NJ Attorney General*

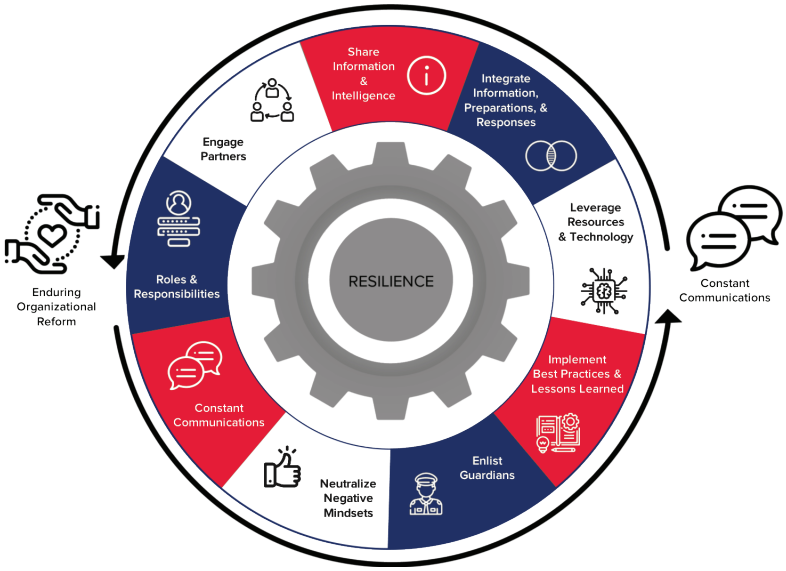
Leadership: Who's in Charge? Of What? When?

Frequently, the head of the congregation takes ultimate charge of all security and communications matters. However, alternative approaches include the elevation of the Director of Security or Chief Security Officer to make security decisions. This delegation of authority can range from all security preparations and responses to only during crisis. During a crisis or an emergency situation, someone must be in charge with full authority to act and direct. Clear lines for who is in charge, in steady state and crisis, are critical.

Take Action!

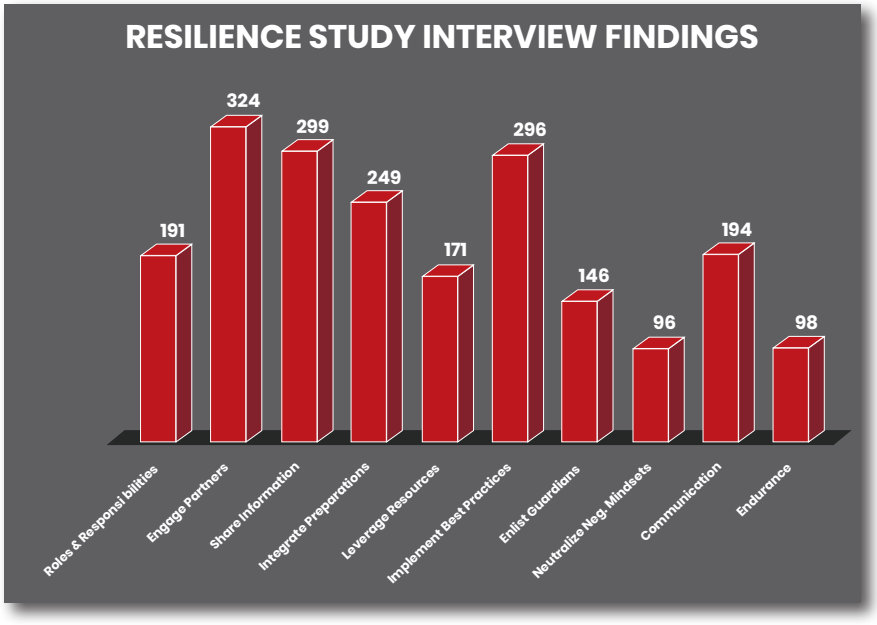
- Institution: Assign Roles and Responsibilities.
- Institution: Coordinate Roles and Responsibilities with External Stakeholders.
- Individual: Know One's Roles and Responsibilities.
- Individual: Know Who is Responsible for What, When.

> *Someone at the house of worship or charity should be aware of the risks they are facing. Someone should have that charge.*
>
> *- Andy Jabbour, Cofounder, FB-ISAO*



PRINCIPLE 2: ENGAGE PARTNERS

The second principle of the RESILIENCE Model is "Engage Partners." Its focus is on building partnerships and creating relationships, within the congregation and community. It is about engaging local partners, state stakeholders, and Federal organizations. By engaging partners early and often, trust and understanding are built. These connections unify individuals, institutions, and communities against common threats. Threats that may be criminal in nature or ideologically driven. The analysis of the 31 formal interviews overwhelmingly demonstrates the importance of engaging partners for houses of worship. Of the ten principles, "Engage Partners" was identified by all of the interview participants and discussed 324 times. As shown in the graph below, at 324, it is the highest count in the study. "Engage Partners" sits at the core of the RESILIENCE Model. It serves as a principle that enables the implementation of the other nine principles. The bottom line is that without partners and relationships with a broad range of stakeholders, the risks to houses of worship are exponentially higher.



> *Relationship-building makes for stronger communities; it makes for safer communities.*
>
> *- Michael Masters, National Director, the Secure Community Network*

Importance

Engaging partners is critical for building resilience within houses of worship and the surrounding community. Not only was it identified 324 times in all 31 interviews, but it was also emphasized by multiple panelists and speakers at Rutgers University conferences focused on building resilience in the new threat paradigm. A paradigm that recognizes the full range of disruptive events for a house of worship, from active shooters to natural disasters. One speaker noted that by creating good relationships with good people, it is easier in bad times to mitigate, respond, and recover. Do not wait to pick up the phone, and do not wait until there is a crisis. Houses of worship are fortunate to have a natural link to a broad range of partners who are willing to support and want to help. They just need to be engaged and invited into your community. Frequently, the enduring gap is a systemic failure to reach out, to connect, and to engage natural partners.

Partnerships have never been more critical, especially in an age of expanding violent extremism. Partners are critical before, during, and after a crisis. Before an incident, building bridges with local first responders, as well as the broader community, establishes a natural exchange of information on crime and threats. This enables security and safety planning. During an incident, these partnerships can ensure rapid, coordinated responses in time-sensitive situations. After an incident, partners help houses of worship recover and reconstitute their capacity to provide services. Panelists from Rutgers resilience-focused conferences consistently noted that at times, the hardest part of dealing with an act of violent extremism is the aftermath, when there is a struggle to explain the tragic loss of life, recover to a new normal, and the need to change security protocols.

Identify, Index, and Optimize Existing Partnerships

> *"There's real value in networking with other faiths, and obviously they do have different religious beliefs, but in terms of security issues, and how to protect your houses of worship, there are a lot of commonalities that I think they can really profit from talking to each other about."*
>
> *- John Farmer, Former NJ Attorney General*

The first step is to identify, index, and optimize existing partnerships. The second step is to then expand on these partnerships, both internally and externally. In the first step, identify and index all of the institution's current partners who may be part of the congregation, broader community, or first responder community. These partnerships may be with other philanthropic organizations, local law enforcement, or internal ushers. Once indexed, take note of strengths and potential gaps in the network of partnerships.

Assess how to optimize existing partnerships to enhance the mission, safety, and security of the house of worship and the broader community. Engage existing partners and keep them informed. Establish regular contact through services, calls, and social events. If the process to identify and index existing partners reveals significant gaps, the key is to start engaging internally and externally. Based on the assessed shortfalls, identify and engage the partners that will have the biggest impact on the safety and security of the community.

Expand Partnerships Internally

The next step is to expand upon existing partnerships, both internally and externally. Internally, within the congregation, there is invariably a wealth of untapped knowledgeable people of faith. Members of the congregation who may be doctors, law enforcement officers, or communication or cyber experts. Often times, these individuals are only too willing to participate but were never asked and did not have a sense for how they could help. Identify these people and ask for their support. Then ask these experts who else within the congregation or external to the house of worship might be willing to volunteer or partner. Mobilizing internal partners creates a more resilient, unified, and aware community. A community that can better prepare for, avert, and recover from acts of violent extremism. Practicing safety and security is a team sport.

> *"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."*
>
> *- Russ Deyo, Former Deputy Secretary, U.S. Department of Homeland Security*

Expand Partnerships Externally – Locally, Federally, and Internationally

With existing partnerships optimized and internal ones expanded, the next piece is to engage external partners. Many houses of worship exist within an ecosystem of untapped external partners. External partners include other houses of worship, community organizations, local first responders, and where applicable, state and Federal organizations. This effort to engage external partners can pull communities of faith together. It can unify a natural ecosystem of like-minded congregations. It fosters an exchange of best practices and lessons learned. In times of crisis, houses of faith naturally show unity, provide mutual support, and facilitate each other's recovery.

At the local first responder level, members of the study recommended easy-to-do events like "coffee with a cop" or "tea with the chief." Events like these build mutual awareness and trust within the community. The Director of Security, as identified in principle one, is likely the ideal liaison with the first responder community. For example, the Director of Security would meet with law enforcement to discuss crime trends and any direct threats to houses of worship.

In addition to local police, it is important to have partnerships with the broader first responder community. These include emergency medical services and the local fire department. Invite them in to review assessments, security plans, and safety protocols. Doing so informs their response efforts in the event of an incident. It affords first responders an opportunity to support the planning efforts captured in principle four, "Integrate Information, Preparations, and Responses."

When possible, research, review, and engage current partners to identify potential relationships at the state and Federal level. For example, the Office of Infrastructure Security at the U.S. Department of Homeland Security is a Federal partner with training and field resources. Field resources include Protective Security Advisors (PSAs) who advise and assist the private sector, critical infrastructure operators, and houses of worship on security matters.

In many cases, houses of worship have natural ties to international systems, organizations, and communities that are ready to support. Meet with partners nationally as well as internationally. These exchanges can be the product of security conferences or from the expanded set of local partners. They can facilitate a further exchange of threat trends and best practices. Engaging with international partners can not only assist in the sharing of information about rising threats, but can also build a sense of unity grounded in timeless traditions.

Institutional Partnering

Part of the tenth principle, "Enduring Organizational Reform," is to ensure that these partnerships are institutional rather than personal. Relationships and partnerships dependent upon specific personalities are difficult to sustain. They are easily disrupted by routine personnel changes or the natural movement of families to new communities. While many relationships will logically grow from and be fostered by personal relationships, over time the codification of these exchanges into an institutional process with the appropriate supporting structure is essential.

Form a Coalition or Join a Faith-Based Council

If one does not yet exist, form a coalition between partners in law enforcement, schools, and fellow religious leaders to discuss common ground. Create a coalition of the willing who are bound together by a common mission and set of values. It takes a network to beat a network.

In addition, join the Faith-Based Information Sharing and Analysis Organization (FB-ISAO). Unify under the mantra that an attack on one house of worship is an attack on all. Build resilient interfaith relationships. These engagements support information exchanges that can increase safety and security by ensuring reporting and investigation of suspicious activities, and that all partners are aware of the current threat picture.

> *Houses of worship should be building relationships with those in their community. They should have a responsibility on them as well to be an active participant in their own well-being. They should know the organizations around them.*
>
> *- Andy Jabbour, Cofounder, FB-ISAO*

Background for Partners Engaging Communities of Faith

- Understand the invariable tension between security measures and the primary mission of houses of worship.

- First responders who are already members of a religious community may serve as initial points of contact to create or strengthen community relationships.

- Be aware that religious facilities often publicize their meeting times and locations, including services and events such as festivals, picnics, concerts, special services, classes, or training. This information can be potentially useful to a terrorist or criminal.

- First responders and religious groups may not have the same level of understanding or a common lexicon regarding violent radicalization. Religious groups need training with law enforcement to promote a common understanding of the indicators of radicalization or mobilization to violence.

- Be aware of how international issues may affect the religious communities within jurisdictions, adjacent communities, or regions.

- When possible, engagement should take place within a wider social engagement context and address issues such as discrimination, criminal activity, or access to social or economic support programs. Engagement can also be facilitated through outreach related to general safety, such as security seminars, fire prevention inspections, and security-system testing.

- Jurisdictions should support and promote outreach groups, such as interfaith councils, to build networks, provide education, and share accurate information on threats and attacks.

- Congregations may negatively perceive the physical presence of first responders and security personnel, especially in uniform. Consider developing alternative, nontraditional, or low visibility means to conduct engagements.

- Religious gatherings may occur in nontraditional houses of worship, such as movie theaters, office buildings, schools, and in homes. These locations may not have standardized or modernized security, including communications equipment.

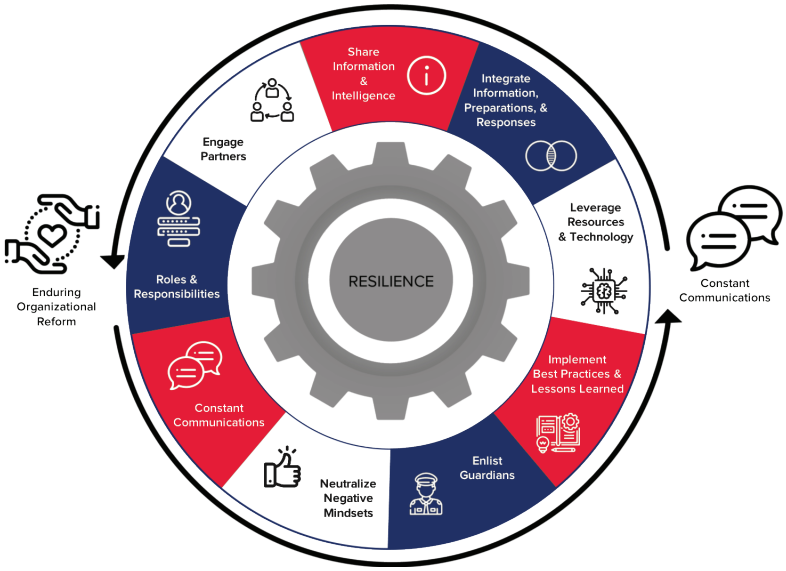
- Religious facilities may run or host activities at venues that provide a public service, such as schools, day and after-care centers, donation sites, and food banks. Special faith-based events may occur in nontraditional venues such as parks or on city streets. Some religious facilities or structures may be tourist destinations with a limited security presence.

- Services or ceremonies may involve separation practices based on gender, culture, age, or other factors. It is important to be aware of specific community sensitivities that may affect the ability of partners to aid during an incident.

  (Source: Joint Counterterrorism Assessment Team)

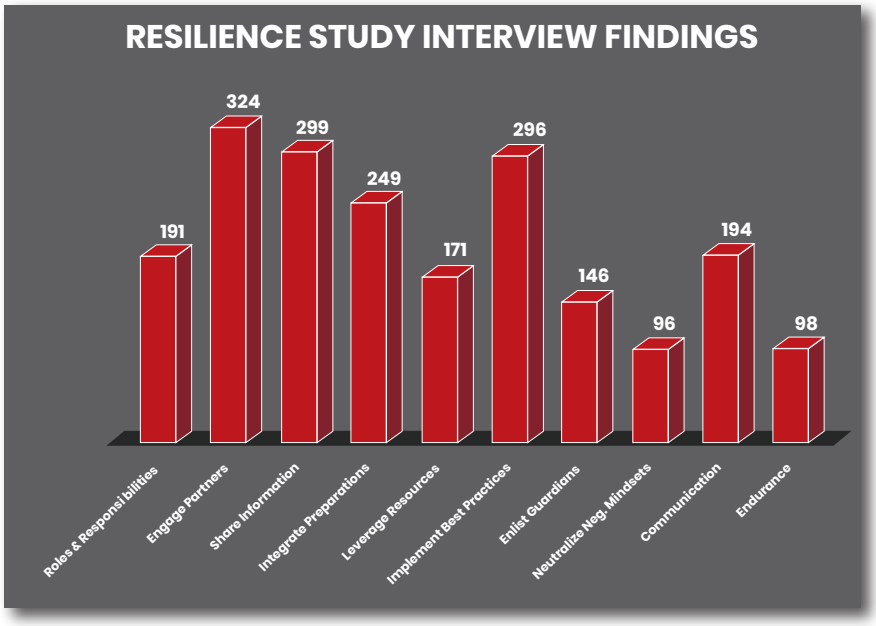
Take Action!

- **Engage Partners.**
- Identify, Index, and Optimize Existing Partnerships.
- Engage Internal Partners.
- Engage External Partners.
- **Build Relationships.**



PRINCIPLE 3: SHARE INFORMATION AND INTELLIGENCE

The third principle of the RESILIENCE Model is to "Share Information and Intelligence." The goal of the third principle is to build situational awareness that enables action! Action that deters, denies, or defeats the actions of potential threat actors intent on attacking a house of worship, the congregation, or community. These actors range from criminals to ideologically driven cyber terrorists. The exchange of threat information is vital to the security and safety of the community. Gathering and sharing information helps mitigate the threat, build connections, and buttress vulnerable communities and houses of worship in times of crisis. It builds awareness and mutual trust.



All of the interviews repeatedly raised the import of "Sharing Information and Intelligence." 100% of interview participants, unprompted, initiated a discussion on how critical it is for houses of worship to "Share Information and Intelligence." Per the analysis of the 31 formal interviews, "Share Information and Intelligence" was identified and discussed 299 times (the second highest count as shown in the graph).

Relationship Between Principles. "Sharing Information and Intelligence" focuses on the need to gather, analyze, and share potential threat information. It is a key driver of principle four, the "Integration of Information, Preparations, and Responses." It is also enabled by and through the second principle, "Engage Partners," and the ninth principle, "Constant Communications."

For houses of worship, this principle is focused on information rather than traditional intelligence. The RESILIENCE Model was developed to be applicable to a broad range of private sector users. For private sector users like a large critical infrastructure owner, operator channels to facilitate the passing of traditional intelligence may exist. However, for houses of worship, the focus is on information sharing, as traditional intelligence will rarely be available or passed on directly.

> *We need to share and disseminate information about the threat. We need to emphasize the importance of cooperation between law enforcement, the public, and the community, especially potential targeted communities and faith-based leaders and organizations.*
>
> *- Ali Soufan, Former FBI Agent*

The Importance of Sharing Information

> *I think that we have a multidimensional picture that's operating through various vectors, and it's becoming increasingly complex to counter those threats. It requires a real sense of awareness among our public safety professionals and first responders as well as within the community itself.*
>
> *- Michael Masters, National Director of the Secure Community Network*

The need to share information on potential threats is likely intuitively obvious. However, how to do it and with whom may be more obscure. On the "who" front, houses of worship need to share information internally and externally. Internally, the Head of the Congregation, Director of Security, and Director of Communications need to create a two-way flow of information with the members of their community. Members of the community need to be empowered to share information and trained on suspicious reporting. Externally, houses of worship need to routinize communications with external partners. These partners include first responders, community organizations, and other houses of worship. Irrespective of different beliefs and backgrounds, houses of worship need to work together to ensure their mutual safety and security. Information sharing is a critical first step in making these connections. The mechanism may be bilateral, directly with another house of worship, or it may be through an interfaith council. Both offer a mechanism to share experiences, best practices, and threat information.

Three-Step Information Cycle – Gather, Analyze, Share (GAS)

The GAS information and intelligence cycle consists of three steps: Gather, Analyze, and Share. The GAS acronym is a streamlined version of a more complex, traditional, and multi-step intelligence cycle that is contextually bound, cumbersome for smaller institutions, and a poor fit for houses of worship.

Gather Information. Information should come from multiple sources, mediums, and partners. This should include internal and external sources, ranging from the institution's own community and local police to faith-based councils and Federal agencies. Collectively, this information should provide the best possible awareness of threats and crime trends. It is also the material for the next step: analysis.

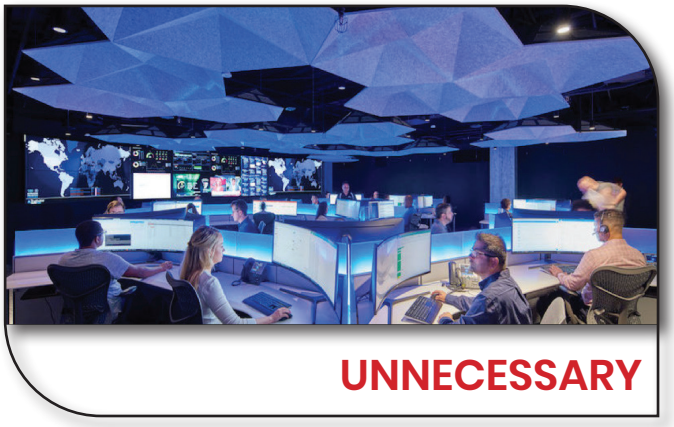
Note: Everyone is an active gatherer of potential threat information.

- See Something, Say Something.
- Suspicious Activity Reporting (SAR).

Analyze the Information. Make sense of the information for your team, partners, and congregation. Assess the information's credibility and value. Is it helpful? Identify the "so what?" What action, insight, or sense of awareness does this inform? Integrate the latest information from multiple sources, mediums, and partners, and add context when possible.

Share Information. Distribute information internally and externally with partners, team members, and the broader community. Share constantly and consistently with the broadest possible audience. Houses of worship and the broader community are interconnected and interdependent.

Reduce Complexity. Just as the GAS acronym is a streamlined version of a more complex, traditional, and multi-step intelligence cycle, the enactment of the principle need not be overly complex. Developing and executing an information process only requires a table, a place to meet, and the right partners. The idea that a more complex and technology-heavy infrastructure is needed is categorically false. State-of-the-art programs and flat-screen monitors will not necessarily make a house of worship more aware or secure. In addition, it needlessly creates a barrier to entry. The key is to reduce entry thresholds that delay or prevent action or forward progress.



UNNECESSARY

NECESSARY

Precision and Accuracy. The sharing of information about potential threats must be timely, but also accurate. The spreading of false information, needless alarms, or information without appropriate context degrades the resilience of a community. Accurate information from reliable sources builds resilience. It directly enables the fight against misinformation. The goal is agility and accuracy.

> *There is real value in networking with other faiths…there are a lot of commonalities, and they can really profit from by talking to each other about those challenges.*
>
> *– John Farmer, Former NJ Attorney General*

Social Media and False Information. Houses of worship should explore the full range of potential communication mechanisms to rapidly and accurately share information. These range from in-person meetings and teleconferences to social media. The evaluation should focus on speed, reliability, efficacy, and the security of the platforms. It should also evaluate the risks associated with false information. For example, social media platforms enable fast and broad dissemination of information. When the information is accurate and used in the right channels, it can significantly help an institution communicate quickly. However, it can also become a mechanism that rapidly passes false information that can build momentum. It can transform minor stories into major stories, where fact and fiction intertwine into a self-perpetuating narrative. A problem that can magnify in times of crisis. Untangling this knot is a key responsibility of the Communications Director, who will ensure the congregation's awareness of misinformation and facilitate a balanced use of social media.

Establish Threat Communication Programs. To open the pathways for information sharing, establish situational awareness and threat reporting protocols and programs. Implement protocols that allow members of the community to communicate concerns, suspicious activity, and potential threats. This can include internal, local, state, or Federal Suspicious Activity Reporting (SAR) programs. Houses of worship can leverage these existing programs to serve as guides for their own initiatives to communicate with their congregation and partners.

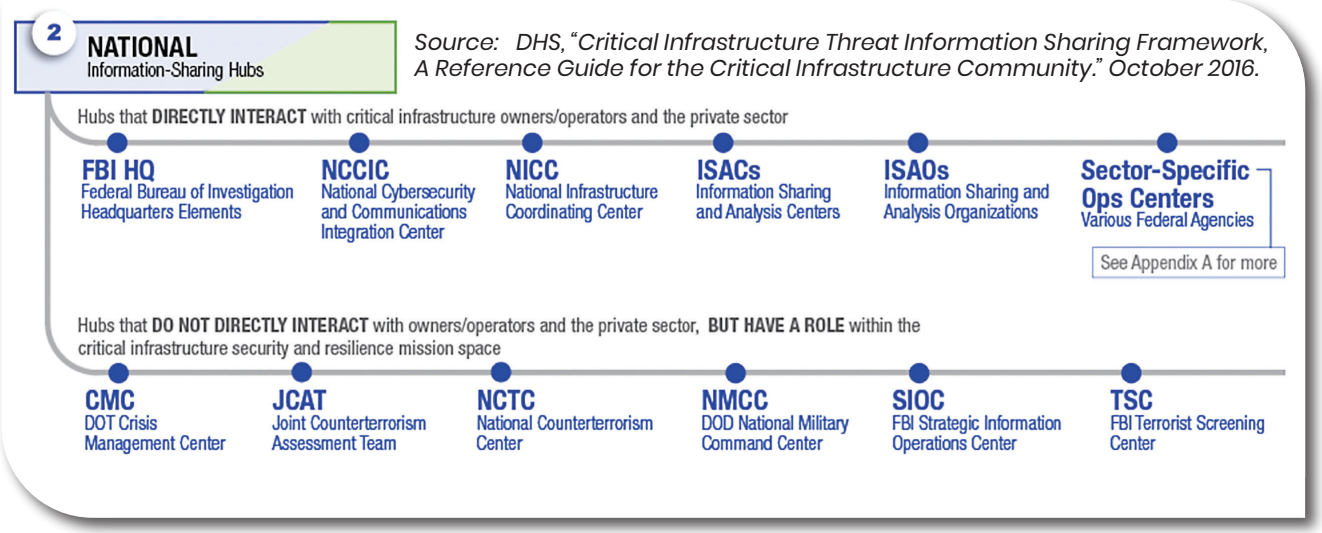
The SAR program, or Suspicious Activity Reporting, is part of the Nationwide SAR Initiative, or NSI, which is run by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and law enforcement. It enables the sharing of suspicious activity. It serves as a means to gather threat information, assess it, and act. The program helps law enforcement to better understand the threat and how to mitigate risks.

Vulnerable communities can also implement their own programs using readily available and low-cost technology. For example, smartphones are largely ubiquitous across most communities and only a simple set of protocols and telephone numbers need to be established. Leveraging this existing technology can enable the effective and efficient identification and reporting of suspicious activity. It allows members to easily connect with each other and share information via text or email. Encrypted communication applications permit a more secure transfer of information internally and externally with stakeholders.

For example, a small house of worship in the southern United States established a straightforward and effective suspicious activity reporting program that helped avert an attack. When a member of the congregation identified a man trying to open locked doors at the church, she immediately called the head of the congregation. Her awareness and the reporting protocol helped sound the alarm. This, in concert with locked doors and cameras, prevented an attacker who would later become an active shooter from gaining access to the house of worship.

Examples of Information-Sharing Hubs

National



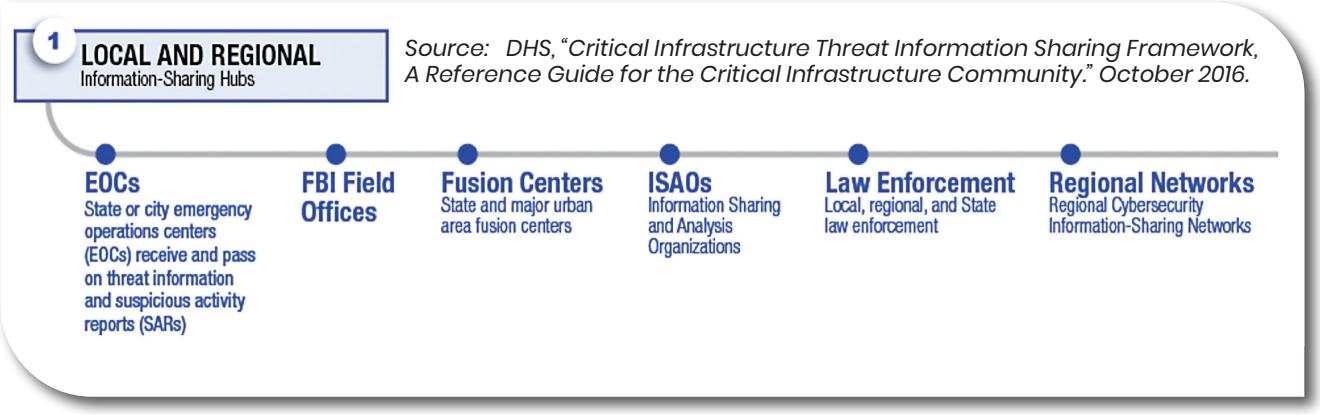
Source: DHS, "Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community." October 2016.

The following hubs directly interact with critical infrastructure operators and the private sector:

- **FBI Headquarters Elements (FBI HQ)**
- **National Cybersecurity and Communications Integration Center (NCCIC)**
- **National Infrastructure Coordinating Center (NICC)**
- **Information Sharing and Analysis Centers (ISACs)**
- **Information Sharing and Analysis Organizations (ISAOs)**
- **Sector-Specific Operations Centers (SSOCs)**

The following hubs do not directly interact with owners and operators and the private sector, but have a role within the critical infrastructure security and resilience mission space:

- **Department of Transportation Crisis Management Center (CMC)**
- **Joint Counterterrorism Assessment Team (JCAT)**
- **National Counterterrorism Center (NCTC)**
- **Department of Defense National Military Command Center (NMCC)**
- **FBI Strategic Information Operations Center (SIOC)**
- **FBI Terrorist Screening Center (TSC)**



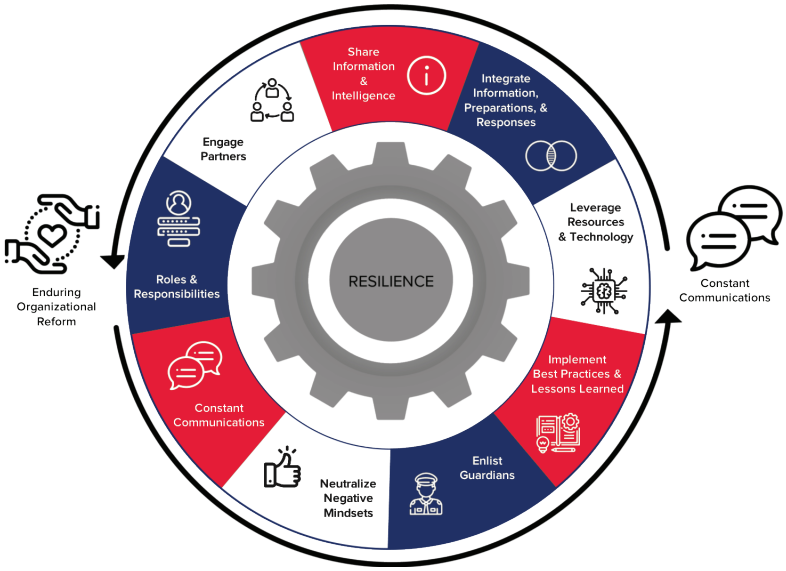
Source: DHS, "Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community." October 2016.

Local and Regional

- **State or City Emergency Operations Centers (EOCs)**
- **FBI Field Offices**
- **State and Major Urban area Fusion Centers**
- **Information Sharing and Analysis Organizations (ISAOS)**
- **Law Enforcement Agencies**
- **Regional Cybersecurity Information-Sharing Networks**

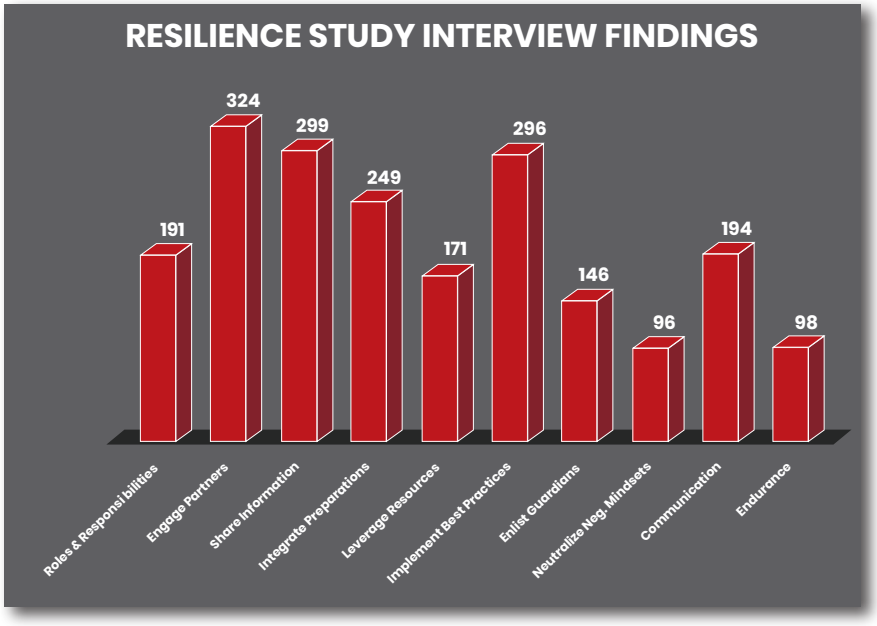
Take Action!

- Commit to the Sharing of Information.
- **Gather Information.**
- **Assess Information.**
- **Share Information.**
- Join FB-ISAO.



PRINCIPLE 4: INTEGRATE INFORMATION, PREPARATIONS, AND RESPONSES

The fourth principle of the RESILIENCE Model is "Integrate Information, Preparations, and Responses." The centrality of this principle is at the core of the RESILIENCE Model. It was noted and discussed in 31 formal interviews 249 times, by 100% of the research participants. It was further noted and remained a central theme in more than 130 informal interviews, conferences, and engagements. The fourth principle is a key gear that leverages the efforts and impact of the other principles and becomes a key driver for the institutionalizing of a culture of security. It is also one of the broadest principles that covers plans, training, exercises, and crisis response.



> *There have to be crisis management plans, and they have to be coordinated, between authorities – across and between faith-based communities and the authorities.*
>
> *- Jonathan Fischer, Former House of Worship Head of Security (Copenhagen)*

Information-Driven Preparations and Responses

With roles established, partners engaged, and information sharing in place, it is time to create information-driven preparations and responses. Preparations include planning, training, and exercising. Timely and relevant information should drive the execution of all of these core tasks. Information on the latest threats helps prioritize training and focus planning. If a set of credible information indicates a significant cyber threat, then this should drive a rapid assessment and planning effort. This cyber threat is now a high probability and potentially high impact event.

If an institution is not integrating information from their partners into their preparations and responses, then it is accepting unnecessary risk. Resilience is dependent upon awareness and action. Partner engagements and information sharing provide that critical dimension of awareness. Awareness of the threat, the environment, and best practices. However, absent action that integrates these critical insights, an institution will not be more resilient. Houses of worship must act to be successful, to ensure resilience in the face of an increasingly complex and chaotic threat environment.

Preparations — Key Concepts

- **You Must Assess to Achieve Success.** Assessment is the first critical preparation step. To chart the course to a more resilient future, an accurate starting point is vital. The assessment should address the ten principles of the RESILIENCE Model, whether using this model or another methodology. The scope of the assessment should include both physical and cyber threats. Restricting the process to only physical security is no longer possible. Cyber attacks designed to impact or enable physical security breaches are growing in volume, velocity, and variety. The RESILIENCE Model, when deployed as an assessment tool, enables the conduct of a physical and cyber assessment. The Director of Security or other designated representative can lead the assessment effort.

- **Think Like an Attacker:** Red Team All Plans and Assessments. Assess the veracity of your preparations and potential responses through the eyes of a potential attacker. "Thinking like an attacker" or using a "Red Team" to challenge assumptions, test plans, and force a hard look at readiness will focus future planning efforts. The "Red Team" will explore if a potential assailant wanted to gain unlawful entry — How would it be done? Where are the gaps? What are the greatest vulnerabilities?

- **Identify and Disrupt the Reconnaissance Phase:** Adversary Signatures. The FBI's systematic review of active shooter events within the United States found that a significant number of active shooter events included a distinct reconnaissance phase. During this period, the attacker attempts to sketch out a plan of attack. It often includes observation and an effort to gain human intelligence. The observation part may include driving by the facility and posting statically, in a vehicle or on foot, to note patterns of movement and security protocols. Remote observation is frequently complemented with a classic engagement of members of the community to better understand security protocols. Often times, the asking of questions that initially appear innocuous, upon reflection, may reveal a more insidious intent.

    - For example, in a tragic attack on a house of worship in the Midwestern United States, the perpetrator conducted an elaborate reconnaissance of the institution. It included an assessment of the exterior of the temple and the surrounding parking

lot. The reconnaissance phase also included a full walkthrough of the temple complex, which was facilitated by a welcoming and inclusive congregation who mistook his interest as benign. A gap in perception and assessment can prove deadly.

- The FBI's review further noted that in cases where a distinct reconnaissance phase is not present, it is often times because the perpetrator worked, lived, or visited the community or institution previously. This "insider threat" has less of a need to do classic stand-off observation as he or she already knows the floor plan, knows the people, and may know the security program in many cases.

- Note that the reconnaissance phase and the effort to develop human intelligence also create a distinct signature. When noted by aware personnel who act on these anomalous behaviors, it can lead to disruption directly or indirectly. Vigilance, presence, cameras, and simple door locks are powerful deterrents.

Assessment Timing and Execution

- Think of assessments as a constant process that enables awareness and action. Build a security culture grounded in a constant review of its plans, policies, and programs. On a daily basis, conduct real-time reviews of what is and what is not working. Every month, look back at the last 30 days and then look forward 30 days. Identify what worked, what needs to be improved, and what could be done better. Act on these insights and integrate them into your plans. Daily and monthly assessments inform and shape annual reviews that look holistically across the organization – physical and cyber. Thinking of the assessment process with the RESILIENCE Model as a cycle begs the question of what options exist to codify a set of assessment protocols.

- **Annual Assessments**
  - Many institutions rely upon an annual assessment. Annual assessments provide a routinized pattern where each year, a single month is designated for its conduct. This affords the opportunity for 50 weeks of execution and continual improvement: security teams spend one month assessing and use the other eleven months to implement best practices that rectify discrepancies and fill gaps. Annual assessments should be complemented with event and threat-driven assessments. An annual assessment today must focus on both physical and cyber threats.

- **Odd / Even Years (Physical / Cyber)**
  - An alternative to the annual physical and cyber assessment is to rotate the annual assessments between physical and cyber-focused reviews. In the first year, the institution selects what it believes to be most vital – physical or cyber. In the following year, there is a shift to the opposite. Thus, if the institution conducts a physical assessment on even years, it will execute a cyber review on odd years. As with annual assessments, this alternating physical and cyber approach can and should be augmented with event and threat-driven assessments as needed. Another approach is to spend the first six months assessing and implementing best practices for physical security, and then in the next six months, shift the focus to cyber threats.

- **Event-Driven Assessments**
  - Event-driven assessments are critical. As the situation, context, and variables change, so must an institution's security assessment and action plan. The completion of an annual assessment and the disciplined implementation of findings is an essential foundation. However, this foundational work must be complemented with assessments focused on critical events within the community. For example, special holidays and large public gatherings warrant a separate analysis. This need not be an elaborate effort, but rather the agile application of the RESILIENCE Model's ten principles that build upon existing work. For example, a review of principle four, "Integrate Information, Preparations, and Responses," will help an institution review current plans and assess needed modifications to ensure safety and security. In addition, a review of principle six, "Integrate Best Practices and Lessons Learned," forces a review of past holiday plans and execution. Have lessons learned from last year been integrated?

- **Threat-Driven Assessments**
  - Threat-driven assessments are a central part of building a culture of security. These assessments can be driven by general or specific threat information that can range from active threats to impending natural disasters. They can also be driven most urgently by specific actionable information that is assessed with high confidence to be credible. A mechanism for responding to actionable intelligence must be identified, especially since this type of information may reach houses of worship in the eleventh hour.

  - **General Information and Intelligence Assessments** are conducted in response to information that is not specific, but represents a change in the threat from the latest review. An example is a situation when a foreign terrorist organization publishes the tactics, techniques, and procedures for using a vehicle as a weapon. Then a vehicle attack is executed with tragic consequences, and indications are that this could become a new trend. If the next special holiday or large gathering is held in a space with viable vehicle access points, a countermeasure review is warranted. Measures might include the introduction of vehicle bollards or strategically parked vehicles to prevent access.

  - **Specific Information and Intelligence Assessments** are conducted in response to increasingly focused and expanding threat information. The specific, direct call for attacks against houses of worship could justify a review, especially when the call for attacks manifests into actual attacks at home or abroad. This may increase the urgency and frequency of the assess and act cycle.

  - **Actionable Intelligence** means a credible and specific threat against a house of worship or the broader community. Here, the intent and capability of the adversary are assessed to be credible. The body of evidence is collaborated through multiple sources and the potential for an incident is high and likely near term. Part of crisis response is to rapidly re-assess current security postures in the face of clear and credible threats. How can the institution rapidly "Engage Partners" to enhance its security posture? To maximize the accelerated "Sharing of Information"? How can the institution pragmatically prevent a tragic event? The intent is to shift the focus to proactive, preventative measures. This is juxtaposed to a focus on reaction and recovery. The intent is to prevent the attack from happening.

- **Complementary or Alternative Assessment Timing**
  - Alternative approaches to the assessment cycle include executing one principle per month or three principles per quarter. These alternative approaches foster a security culture of constant review, facilitate an ever-adapting defensive architecture in the physical and cyber world, and afford a monthly or quarterly focus on a sub-set of the RESILIENCE Model's principles. However, they do present potential logistic and capacity challenges that may strain limited bandwidth for security matters.

- **Deliberate and Rapid Assessment Templates**
  - The Deliberate RESILIENCE Assessment, available on page 70, is a strategic framework developed for annual assessments or odd/even year assessments. The assessment tool delineates point values for each RESILIENCE Model principle. It is intended to facilitate an in-depth review of a facility's preparations and response capability without being overly prescriptive.

  - For event-driven and threat-driven assessments, which are conducted in response to a changing security situation, teams can utilize the Rapid RESILIENCE Assessment. It is available on page 69. This tool is meant to serve as a quick "check-in." One that can be completed by several individuals at once to quickly reassess a facility's state of security and preparedness in the event of an increased threat environment, such as a spike in local crime.

Preparations – Plans from Steady State to Crisis

> *Have a plan, rehearse your plan, and after you've rehearsed your plan, improve your plan.*
>
> *- Kona Zoganas, House of Worship Director of Security*

- **Steady State Plans**
  - **Daily Operations.** The safety and security plans for daily operations form the foundation for all other plans. Think of it as the base plan executed every day. As threats and situations warrant, the head of security or the congregation can make informed choices to adopt standing plans and procedures. It forms a baseline of security and safety procedures that is realistic and repeatable for protracted periods of time.

  - **Special Services and Events.** Special services and events are routinized events that may occur weekly, monthly, or annually within a house of worship. Special event timing is frequently known broadly by members of the congregation, as well as the larger community. Frequently, these events include a larger than average concentration of citizens and warrant enhanced security protocols. This could include increased law enforcement presence, additional screening of attendees, and the establishment of a barrier plan.

  - **Large Public Gathering.** Plans for large gatherings address the need for enhanced safety and security protocols during periods of unique concentration of a congregation or community. These are gatherings that, due to their sheer size and

number of participants, warrant additional resources and planning. These can be events held within primary facilities like a church, temple, or mosque, or they can be gatherings held away from primary facilities at outdoor or indoor infrastructure, like parks or restaurants. A separate plan should be drafted, reviewed, and integrated with internal and external stakeholders and partners. This is particularly important when large gatherings are held outside of traditional facilities, due to an increase in uncertainty.

- Note: In most cases, large houses of worship are already developing plans that enable the conduct of daily operations and manage large gatherings. The focus here is to simply take what is already being done and add a security review. This review does not need to be exhaustive and should complement existing efforts and procedures.

- **Crisis Response Plans**

  - **Crisis Response Plans.** These plans allow a house of worship to prepare for extremely disruptive, yet infrequent, events. These are plans for high consequence, but low probability events. House of worship crisis response plans include fire evacuation, active threat, improvised explosive devices, and natural disaster. Crisis response plans are distinct in their need for precision and coordination, the compression of time, and consequences. For example, the FBI's review of over 160 active shooter events demonstrates the extreme compression of time. In their review, the vast majority of active shooter events end within a few minutes, and many end before law enforcement can arrive on the scene. Well-thought-out, coordinated, and rehearsed crisis response plans are critical for rapid action when seconds count and translate into lives lost or saved.

Contingency Plans

- **Succession Plan.** Succession plans ensure the continuity of critical personnel in support of the safety and security of a house of worship. These plans cover the anticipated transition of key personnel, to the loss of or lack of access to critical players at the point of crisis. The succession plan identifies a primary, alternate, and tertiary lead for security and communications. If the security lead moves to a new location, the designated alternate would fill the vacancy. On the other end of the continuum in crisis, if the primary communications person cannot be reached, the alternate assumes the position.

- **Communications Plan.** Speaking with one voice before, during, and after crisis is essential. With the first principle, the role of the Communications Director was identified and filled. This person will serve as the lead for developing the steady state and crisis communications plan. It will address key basics that include: Who is communicating? What are they communicating? When? Why? The plan will routinize communication channels internally and externally. Such standardization increases the flow of accurate information. At a point of crisis, it enables more agile responses, improves coordination, and reduces friction. During an emergency, the goal is to avoid errant communications, everyone or no one talking, and the dissemination of false information, which all increase uncertainty. Increased

uncertainty only compounds the invariable chaos of the event, which all further degrades responses. In this day and age, to not have a communications plan is tantamount to accepting chaos in crisis. Note that these plans need not be overly complex.

Awareness Plans. Sense It! Identify Suspicious Behavior! Push Out Your Perimeter!

- Awareness plans empower every person to be part of the broad continuum of safety and security plans. A plan to mobilize and empower every member of the congregation to be aware, to identify and report potentially problematic behavior and indicators, is critical. Absent a plan, all too often the potential power of the people is never mobilized. People want to help, but they need a plan. They need a pathway to channel their contributions and support. The integration of simple technology and protocols can bring this to life. Leveraging ubiquitous smartphones, with multi-modal communications capabilities, provides a simple solution that is already fielded. It only takes an awareness plan to transform potential into real capability. In addition, a smartphone paired with one of many potential applications can provide an even more tailored and specific solution.

Natural Disaster Planning

Just as Federal and state emergency management teams conduct annual assessments of community vulnerabilities, so too must vulnerable communities also understand the threats posed by natural hazards. Public health emergencies such as pandemics, biological and chemical accidents, radiological and nuclear hazards, or severe weather events such as winter storms, hurricanes, earthquakes, tornadoes, floods, droughts, and wildfires all contribute to and influence the need for strategies to build resilience. In 2020, our nation, and indeed the globe, has been experiencing the devastating effects of the Coronavirus-2019 (COVID-19) Pandemic. Preparing your organization and community by reviewing the U.S. Center for Disease Control (CDC) guidelines helps everyone mitigate the magnitude of the consequences. Following the RESILIENCE Model principles can assist with developing individualized protocols for organizations to safeguard and prevent loss of life.

Key Factors to Consider for Natural Disaster Planning:

- Size and scale of natural disasters can be significantly larger than other threat events (think Hurricane Katrina, Super Storm Sandy, or COVID-19).
- Duration of natural disasters can be significantly longer.
- Impact on critical infrastructure can be significant and lasting (think power, water, road, and bridge infrastructure).
- Impact on supporting infrastructure can also be broad and enduring (think access to gas, groceries, and good jobs).
- The need for houses of worship services will only expand, while infrastructure, resources, and the core team may all be severely degraded.
- When planning for natural disasters, think whole of community. A house of worship is not an island unto itself.

- Understand your congregation and community and tabletop the preparations necessary to provide enduring services in the darkest of hours (think understanding demographic characteristics to best prepare for what a unique community will need most).
- Understand the intergovernmental and interagency emergency management system in times of natural disaster.
- Understand the relationship between Federal, state, and local government support.
- Develop contingency plans that enhance ongoing efforts to care for those most in need, in an austere environment (think food, shelter, medical care, in addition to traditional spiritual needs).
- Be prepared to adapt traditional services to a rapidly changing environment (think COVID-19 virtual services and Katrina park services).
- Think Prevention, Protection, Mitigation, Response, and Recovery for Natural Disaster Planning.

Clark Rapid Planning Process – *Clark Assess-Plan-Act (CAPA)*

Why Do We Plan? We plan to prepare. We plan to align limited resources against prioritized threats, challenges, and opportunities. The CAPA planning process enhances situational awareness, the understanding of the problem, and the range of practical solutions.

> *Planning is the art and science of envisioning a desired future and laying out effective ways of bringing it about.*
>
> *- Marine Corps Doctrinal Publication (MCDP-5) Planning*

How Do We Plan? The Clark Rapid Planning Process for communities provides a repeatable and simple three-step process. The first step is to assess, the second is to plan, and the final step is to act! Complexity in planning is the enemy. Complexity is a barrier to entry and an impediment to action and implementation. A streamlined, simple, and straightforward process is needed. Planning processes designed for large corporations or government entities are authentic and relevant to those institutions, but often do not translate or transfer to houses of worship.

Step 1: Assess

An enduring best practice noted throughout this work is the need to conduct assessments, which also serve as the first planning step. Assessments enable a shared understanding of the problem and promote situational awareness. They help build a map. Assessments identify threats, challenges, resources, strengths, and weaknesses. They reinforce what is going well and identify gaps that require further review.

Step 2: Plan

Step two takes the assessment and builds ways to address security gaps and reinforce strengths. This planning step consists of three key parts: Build, Review, and Select the best option. The first part is to build potential options that solve the problem or gap identified in the assessment. Part two is to review those options, and part three is to select the best option.

Step 3: Act

The final step in the CAPA planning process is to "ACT!" The planning process is deliberately restricted to three straightforward steps in order to ensure a focus on action. Once an option is built, reviewed, and selected, the key is to act on its implementation. If the assessment indicates a lack of written and rehearsed plans, then the key action is likely to draft, test, and implement missing plans. The drafting process need not be excessively elaborate. A straightforward bulleted document or slides are fast and easy to develop. In addition, the planning process facilitates coordination with internal and external stakeholders. Plans need to be coordinated with all stakeholders.

Integrated Plans and Planning

- Physical and Cyber Integration
  - A physical and cyber assessment is critical for the development of integrated plans.
    - Integrated across all threats —physical and cyber.
    - Integrated across plans for active shooter to improvised explosive devices to natural disaster.
    - Integrated across cyber attacks ranging from efforts to disrupt to attempts to exploit information and financial resources.

- Internal Integration
  - Plans must be integrated across the internal team to ensure the safety, security, and resilience of a house of worship. Integration is ideally achieved through an inclusive, transparent, and deliberate planning process. This process creates the opportunity to weave together the internal team's best thinking and ensures coordination across the full family of plans.

- External Integration
  - Plans must be externally integrated, as no house of worship, institution, or community possesses all of the internal resources necessary to ensure its organic safety and security. The integration of first responders is essential in the planning process and in the final plan. Ideally, first responders are integrated into the plan as early as possible. If current plans do not include recent coordination with first responders, reach out to fire, rescue, and law enforcement officers today. To be successful, houses of worship must work together with all internal and external partners and stakeholders.

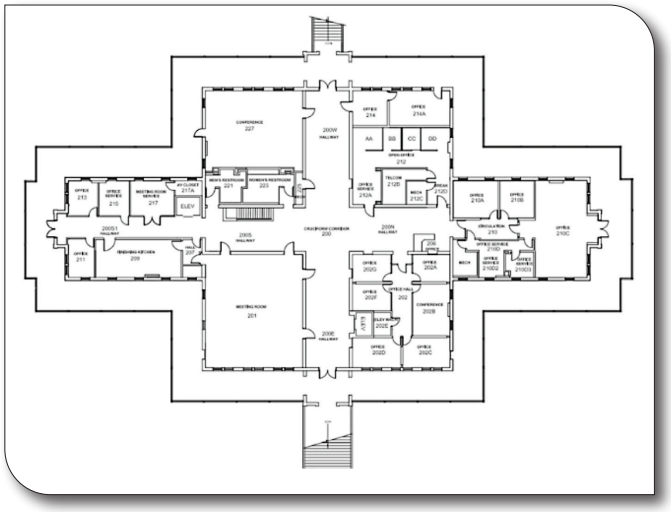
<u>Train and Exercise</u>

Training – *The Three "Its": Sense It, Map It, Lock It (SML)*

- ***"Sense It":* Awareness Training and Technology.** The ability to identify suspicious behavior is vital. Human dimensions training should not be limited to the security director or team, but should be disseminated across the community. Everyone needs to know what to look for, and threat awareness instruction will facilitate enhanced situational awareness. It is also important to note that what may look suspicious in a commercial environment can be normal in a religious environment.

People seek solace in houses of worship that are open to those who may be despondent or depressed. Training for the congregation, greeters, and ushers to identify anomalous behavior must be within the unique context of that specific community. "Sense It" is enhanced through the deployment of technology, such as the integration of cameras and alarms. Training that ensures the right "tech" selection, application, and integration is critical. Poorly understood and wrongly applied technology is of minimal value. Once sensed, key information must be passed on quickly and efficiently. When executed correctly, Suspicious Activity Reporting (SAR) programs serve as a key building block for a culture of security.

- ***"Map It":*** **Integrate, Coordinate, and Execute Plans.** The internal team and the external team, which includes first responders, need a common map to prepare and respond. "Map It" is simple – know where you are and know where we are! All too often, crisis response operations are delayed due to the lack of a common map or system to geospatially locate and coordinate response activities. First responders, the internal security team, and the congregation need a simple, reliable map system. One that identifies entry and exit points, evacuation routes, and safe havens. The key is a shared understanding of a geospatial system that enables a rapid, coordinated response. The system can be an alphanumeric grid system or one that designates every room. Alternatively, it can be based on building blueprints or a separate product developed jointly – so long as the end state is a shared understanding of a map.



> *This summer our school will be mapped … that'll be available to all law enforcement on their phones, in their cars … So instead of trying to say go to room 111 in the middle school, it's a grid point, go to A6. There's a close map and then there's a distant map … it was actually developed by a bunch of special forces guys.*
>
> *- Robert Lake, Middle School Assistant Principal*

- ***"Lock It":*** The bottom line is that locked doors work, and are a timeless security measure. The vast majority of active shooters have not demonstrated the intent or capability to successfully breach doors. A locked door or even one that is barricaded is a significant obstacle. Case studies of active shooter events where doors are locked or barricaded demonstrate the efficacy of this simple but effective technique.

> *I'm a big fan of run, hide, fight. I think it's good to learn, and you should have a well trained and experienced person teach it to the congregation.*
>
> *- Roger Parrino, Former NY State Head of Emergency Management*

Action Focused Training. *Learn to Protect Self, Others, and the Community.*

Active Threat Training: The Department of Homeland Security active threat training includes the concept of "Run, Hide, Fight." It is best to think of "Run, Hide, Fight" as a series of options vice a linear continuum for someone caught in an active threat situation be it a firearm, knife, or vehicle. Based on the situation, one chooses to run, hide, or fight. Run if you can, hide if you think best, or fight if you must. An alternative way to think of this is "Deter, Deny, Defend." Deterrence starts now and is intended to shape the environment to reduce the threat. Deterrence is focused on pre-crisis activities. To deny begins at the point of crisis and includes evading (running or hiding) and blocking (locking doors or barricading). It is the process of actively adding angles, distance, and obstacles between the individual and the shooter.

To defend begins at the point of first direct contact with the adversary. It is focused on the protection of self and others by directly or indirectly engaging the active shooter when other options are no longer viable. For example, during an active shooter event at a school in Oregon state, a veteran of the U.S. Army defended his fellow students by drawing the attention of the shooter and then barricading a door with his body to prevent the further movement of the shooter. These defensive actions allowed his fellow students to evacuate. It bought his classmates time to run and evade!

> *We teach them different active shooter protocols to include: run, hide, fight, and ALICE. Alert, lockdown, inform, counter, evacuate.*
>
> *- Brad Orsini, House of Faith Security Director*

Bomb or Improvised Explosive Devices (IED) Training: IED or bomb awareness and reporting training are essential. In the past 12 months, dozens of IED attacks around the world have killed hundreds of practitioners in their house of worship. To counter this threat, the first step is awareness. The second is to rapidly and reliably report all threats, potential threats, and anomalies. The simple detection of a backpack or box sitting unattended in an odd place, which is then reported, can disrupt a potentially destructive event. IED training is focused on awareness, reporting, and evacuation. "Sense It," "Map It," and "Get Out."

Medical Training: Basic medical training is already conducted by many houses of worship. It often times includes introductory first aid and CPR training. In some cases, it now includes higher-end shock and trauma training. The current threat environment makes it prudent to maintain, or if not in place, to introduce a broader range of medical skills. Integrate the "Stop the Bleed" campaign and the growing inclusion of tourniquets in first aid kits. To make a medical plan work, assess and understand the current skillsets within the congregation. Next, institute the training, internally and externally. With training in place, ensure that the necessary medical equipment is staged and ready for use. Basic first aid kits and trauma response equipment can be staged out of sight, but readily available.

> *"There's zero awareness! People have no idea regarding their significant cyber risks. And worse, people just automatically assume, well, that only happens to big companies. That doesn't happen to us. You know, nobody would care about us. I hear that all the time. Clients have been breached? Well, nobody would care about us."*
>
> *– Brian Dykstra, CEO*
> *Atlantic Data Forensics*

Fire and Arson Training: Fire evacuation plans are relatively standard business for most institutions. However, after action reports are replete with mistakes that cost lives. Chained doors, faulty alarms, and a lack of training are three culprits. Ensure that your fire evacuation plans, routes, and alarms work and are understood by your congregation.

From unintentional fire, now let's explore fire as a weapon, or arson. In the past 12 months, multiple houses of worship have been burned to the ground and the cause has been ruled as arson. Arson attacks involve the focused use of combustible materials to create a destructive fire. Arson can create a violent and even explosive fire that spreads rapidly. The time to evacuate and respond can be dramatically reduced. Plans, training, and exercises conducted in support of standard fire evacuation become the foundation for arson countermeasures. However, there is an extreme compression of time and a compounding uncertainty as to the nature of the event. If the fire is large, spreading rapidly, and started with an explosive-like burst, assume the worst and evacuate as rapidly as possible. Make no attempts to recover artifacts until all members of the congregation are evacuated and first responders are on the scene.

Cyber Training: Training in the physical space often comes more naturally to an organization than the virtual world of the cyber domain. Invariably, the organization may have more experience with training for large events, active shooters, and detecting anomalous behavior. Nonetheless, the need to integrate cybersecurity training is of paramount import.

All institutions and the broader network they communicate and transact with are becoming increasingly reliant upon the internet. It is a space where wealth, knowledge, and personal information are increasingly stored and used. The vulnerability of the internet and increased reliance on its use for all matters is compounded by the sheer volume, variety, and velocity of cyber-based threats. Threats from a range of actors include criminals, terrorists, and nation-state adversaries who are increasingly capable and emboldened, and whose intentions range from exfiltration and exploitation to disruption and destruction.

Preparations today must include cyber plans and training. The first step is always awareness of the threat and their tactics. A range of tactics from sophisticated socially engineered attacks to ransomware. Once aware, the next step is to provide practical mitigation measures and practices. Best individual practices include the following: two-factor authentication, tokens, strong passwords, patching immediately, and identifying and avoiding scams. Best institutional practices include the following: access controls, routine backups of all information, minimizing data storage and removing unnecessary personally identifiable information, deploying a defendable architecture with up-to-date antivirus, firewalls, endpoint detection and other malware tools, strong physical controls to limit computer access, and the active management of email and social media accounts to reduce the attack surface. In addition, institutions need to ensure compliance with an ever-shifting regulatory and compliance cyber framework as directed by the local, state, and national levels.

Exercises: With plans developed and the team trained, it is time to exercise. Exercise the plans, the training, and most importantly, the people. Exercises are critical for testing assumptions and plans. This testing process provides a critical feedback loop for the refinement of plans and the enhancement of future training. Exercises can range from simple tabletop events to full-scale, multi-day, multi-jurisdictional exercises designed to realistically simulate the most difficult of circumstances.

- **Meet and Talk.** The entry point into the world of exercises is simply to meet and talk with internal and external stakeholders. A series of kitchen table reviews of the current situation, standing plans, daily operations, and any future special events will increase readiness. The core requirement is a group of willing and able people who know their roles and who are willing to productively meet in whatever space makes the most sense. These meetings can occur in any number of locations, from a house of worship to the local firefighter house. "Meet and Talks" can be conducted as a series of events that might initially start with internal members and over time, integrate first responders or other members of the broader community.

- **Tabletop Exercises.** The next step is a tabletop exercise, which offers an effective and inexpensive way of testing plans or rehearsing for a special event. Tabletop exercises require more preparation than a "Meet and Talk." However, this should not be a barrier to entry. A single facilitator who walks the convened group through a scenario, testing the plan and associated personnel, may be all that is necessary. On the other end of the spectrum is a full scenario, with multiple steps conducted over a model or map that can last for hours or days. Tabletop exercises allow internal and external leaders and team members an opportunity to work together. The process builds relationships, experiences, and identifies shortfalls to be corrected.

- **Limited-Scale Exercises.** Limited-scale exercises move from the meeting room to the real world. It's a transition from the abstraction of map and model-based exercises to the real-world terrain model. Limited-scale exercises can range from internal security teams doing a walkthrough, to integrated first responders executing their roles and tasks in the actual house of worship, in preparation for a special event. Limited-scale exercises can be as simple as training and exercising with first responders. It doesn't have to involve the full team all at once; partial teams or key team exercises are effective as well.

- **Full-Scale Exercises.** Full-scale exercises are the most complex and logistically intensive option. They are scenario-driven and will include all internal and external participants. For a full-scale active shooter exercise, a house of worship leader, security team, communications team, and potentially other members of the congregation would participate. Police, firefighters, and emergency medical personnel would be responding to the active shooter just as they would if the event were real. Full-scale exercises are an unquestionable best practice. However, a word of caution in that they are the product of a significant amount of prior work in order to make them effective. Once plans are drafted, coordinated, and tested in tabletops and limited exercises, then the move to a full-scale exercise is a logical step.

Best Practice: Draft an Annual Training and Exercise Schedule
Best Practice: Rehearse, Rehearse, Rehearse

Response – Coordinated Action

Integrated and Coordinated Responses. At this point, a house of worship has identified roles, engaged partners, and is sharing information. The security team is now actively building information and intelligence-driven plans and operations. With plans, training, and exercises integrated, the team is ready to focus on responses. Just as information, plans, training, and exercises need to be integrated with internal and external stakeholders, so must the response to an event. All of the training and planning is designed to ensure that the only possible response is an integrated one. Integrated planning, training, and exercising with first responders build the vital foundation for response in crisis – an all-threats approach to threats and response, be it an act of man or natural disaster. The focus of all the partner engagement and integrated preparations is to prevent tragedy and the loss of life. The key is to prepare now and execute those plans if crisis emerges. All of the preparations increase the probability of a coordinated and integrated response. It is essential that while in crisis the identified coordination measures are executed.

- For example, the role of a Communications Director and the responsibility to communicate during steady state and crisis response has been given to a primary and alternate person. The actions of the primary and alternate Communications Directors have been integrated into and tested across the plans, training, and

exercises. External stakeholders know and understand their role and how they will coordinate with these individuals during a crisis. The intent of the planning process is to work these coordination issues out prior to crisis and then to execute those decisions in crisis. Adaption is of course essential, as every situation will demand adjustments. However, the wholesale abandonment of all preparations is dangerous in crisis and disruptive to the responding local, state, and Federal entities.

Citizen as First Responder. This is more than a concept - it is a reality. Whether we prepare for it actively or allow it to emerge in crisis. An elusive predatory threat who actively recons and selects targets where he or she believes they can impose maximum damage forces the average citizen to be thrust forward at an unknown time, place, and role. They are thrust forward to serve as medic, evacuator, and, at times, guardian. Active preparations that prepare citizens to fill the critical minutes before first responders arrive on the scene are essential. In crisis, the informed, prepared, and empowered Citizen First Responder will facilitate a coordinated transition of responsibilities to first responders. They will also continue to support response teams as needed. We need to put time on the clock and Citizen as First Responder is one pathway.

Response Times: From First Mitigation to Recovery

- What is the response time for law enforcement, fire, and medical?
- How does this inform preparations and responses?
- How long will citizens have to serve as a first responders?
- How long will the congregation have to hold out?

> *Know the response times of your first responders.*
>
> *- Andy Jabbour, Cofounder, FB-ISAO*

Finding Balance

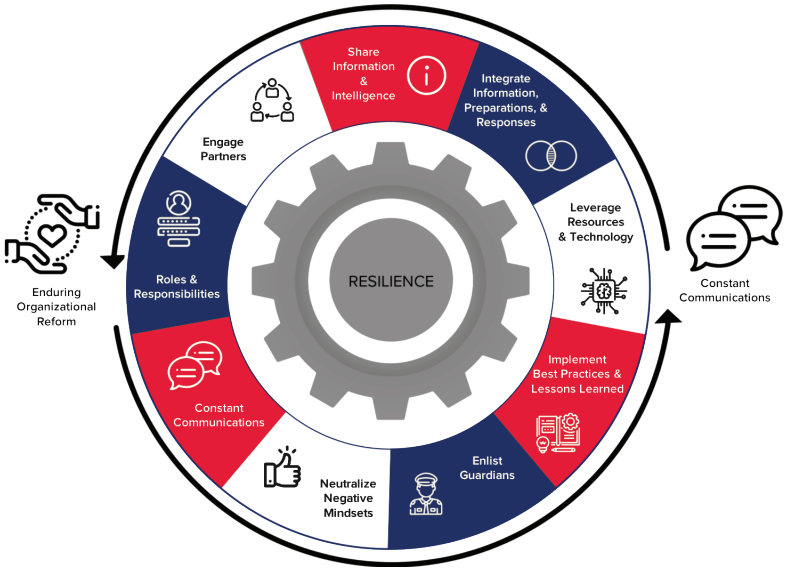
Preparations from training to security protocols need to be in balance with the need for houses to be open and accessible, yet safe and secure. Proactive measures to ensure safety and security should ensure that houses of worship remain open and accessible in perpetuity. Safety and security measures should deter and mitigate disruptive events. A balance must be maintained between the primary mission of the institution and the critical supporting arm of safety and security.

> *I could create you a perfectly safe house of worship, like I could create you a perfectly safe airport, and a perfectly safe city, but they would all be unbearable… a balance has to be struck.*
>
> *- Jeh Johnson, Former Secretary of the U.S. Department of Homeland Secretary*

Take Action!

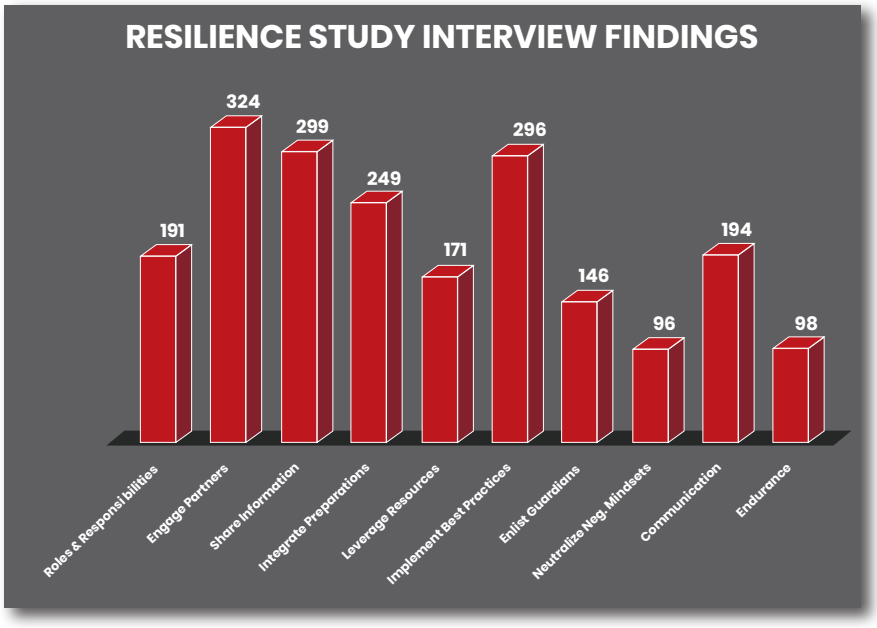
Conduct an assessment and use it to start addressing areas that need improvement. Begin drafting or reviewing plans if already written. Integrate internal and external stakeholders into preparations and responses.

- Conduct an Assessment.
- Draft Plans for Steady State and Crisis.
- Draft Plans Driven and Guided by the Best Information.
- Rehearse the Plan with Stakeholders.
- Train and Exercise.
- Update Plans and Training Based on Gaps Identified During Exercises.
- Integrate First Responders into Institutional Planning and Responses.
- Execute Plans in Crisis / Run the Play.



PRINCIPLE 5: LEVERAGE RESOURCES AND TECHNOLOGY

The fifth principle of the RESILIENCE Model is "Leverage Resources and Technology." It was discussed in all of the formal interviews 171 times. The vast majority of discussions on resources and technology were unprompted and arose naturally by the experts during the interviews. The key to principle five is to map current resources and seek additional ones through public and private organizations to meet security and communication needs. The systematic mapping of potential sources frequently reveals a much larger resource pool. With resources secured, the procurement of low-cost technologies that will significantly enhance security is readily available.



> *Understand the resources you have and the ones you don't, and where you can get them.*
>
> *- Kona Zoganas, House of Worship Director of Security*

Leveraging Resources and Technology – Private and Public

Across the world, there are private and public organizations that focus on assisting houses of worship to increase their resilience and to minimize risks to the congregation. An integrated portfolio of public and private resources not only expands the potential resource pool for a house of worship, but also provides an additional degree of resilience. For example, as access to private funds ebbs, a house of worship with established public grant funding lines can weather this fiscal shift. The converse is of course true as well. As public dollars shift, an active private donor population maintains continuity of funded training, exercises, and security enhancements.

> *Institutions should look to the resources that exist, that are provided to them locally as well as by the Department of Homeland Security and supported by or provided through organizations such as ours, the Secure Community Network.*
>
> *- Michael Masters, National Director of the Secure Community Network*

Public Resources

Federal, State, Local. The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) provide a range of services and tools for houses of worship. From training resources to grants, these entities can assist in creating, sustaining, and improving the physical and cybersecurity of a house of worship. State and local municipalities present an additional layer of resources that can range from funding to direct training.

> *Homeland Security, the FBI have great resources that are readily available with pre-built templates that you can tailor and tweak to fit your organization.*
>
> *- Andy Jabbour, Cofounder, FB-ISAO*

Funding (Grants). Federal and local governments make grants available to obtain training, technologies, and tools that increase the security of the facility and congregation.

Training and Exercises. DHS, as well as state and local first responders, are potentially available to assist houses of worship in providing training and exercises of emergency plans.

Resource Guides and Expertise. Security templates and planning checklists are available on the DHS website in many of the states' security websites. Many agencies have security consultants that are ready and able to answer security or emergency planning questions. For example, the Cyber and Infrastructure Agency (CISA) within DHS has a fully constituted team of Protective Security Advisors (PSAs), deployed across the United States to support the private sector and faith-based organizations with security assessments, planning, and protocols.

> *The Department of Homeland Security offers a Nonprofit Security Grant Program to help nonprofit organizations fund security planning, equipment, training, exercises, management, and administration.*
>
> *- Paul Goldenberg, Senior Advisor, Rutgers University and Private Sector CEO*

Private Resources

Funding (Donors, Sponsors). Global organizations and national nonprofit organizations can provide financial resources to fund houses of worship security measures and training. In addition, fundraising efforts by the local communities offer assistance that is often targeted to solving an important and specific need as soon as possible.

Technology. Private resources can also assist with the acquisition of technology. This can include cameras, new IT equipment, and back-up crisis communication equipment.

Assessment and Plan Support. Private resources can also be invested in enlisting guardians to help assess and secure a facility. These measures can range from bringing in a cybersecurity team to rectify an intrusion to hiring a planning team.

Map Existing Resources: Helping America's Youth and Youth.Gov Example. President Bush launched the Helping America's Youth initiative, and President Obama transformed and expanded the initiative into Youth.Gov. The enduring intent was to identify and elevate evidence-based programs that had the greatest efficacy for positively impacting communities and their youth. An interagency team consisting of the U.S. Departments of Health and Human Services; Justice; Education; Agriculture; Labor; Commerce; Housing and Urban Development; the Office of National Drug Control Policy; and the Corporation for National and Community Service worked together to identify the best evidence-based programs. The initiative also developed an interactive community guide.

The Community Guide includes a community assessment and a resource guide. The community assessment guide is designed to identify youth problems, the people most affected, and what programs exist to serve as part of the solution. The assessment process facilitates the development of a community resource inventory. The inventory captures all of the potential partners and programs in the community. It also provides a visual map that shows the location of all relevant resources and assets. This inventory and mapping process frequently reveals resources and partners that were not previously identified. In a resource-constrained environment, it helps communities to maximize increasingly scarce dollars.

A Community Resource Inventory

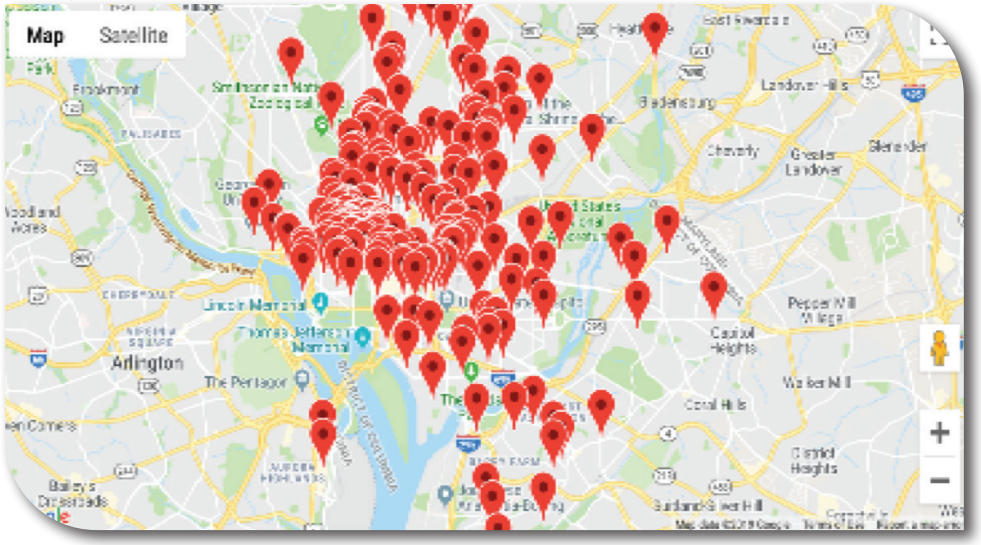
Map It. Map all of the programs and resources in the community that impact, complement, or help your house of worship. From local crime programs to national funding designed to counter the opioid epidemic. Start with a list and then plot them on a paper or virtual map.

Be Aware. Monitor the resources within the immediate and broader community to maximize efficiency and effectiveness.

Integrate / Leverage. Ensure full integration of all available resources. Leverage the congregation's expertise as well as local and national assets to fill critical gaps and maximize resilience.

Reduce Duplication. It is good to have depth; however, it should be decided where to have depth. Duplication might be a sign of inefficiencies in processes or in resources. Aim to reduce unnecessary efforts and to streamline protocols, processes, and procurements.

Evidence-Based. Focus on integrating and leveraging evidence-based best practices, technologies, and protocols. Absent a body of evidence, the simple transfer of a practice or technology from one institution to another comes with no guarantee of efficacy. Resource and security decisions should be based on evidence. When hard empirical evidence is not available, then the robust experience of true security experts should be collectively sought out and engaged to identify the best resource decisions.



Resource map of Washington, D.C. area, capturing all relevant organizations and resources at every level (local, state, Federal)

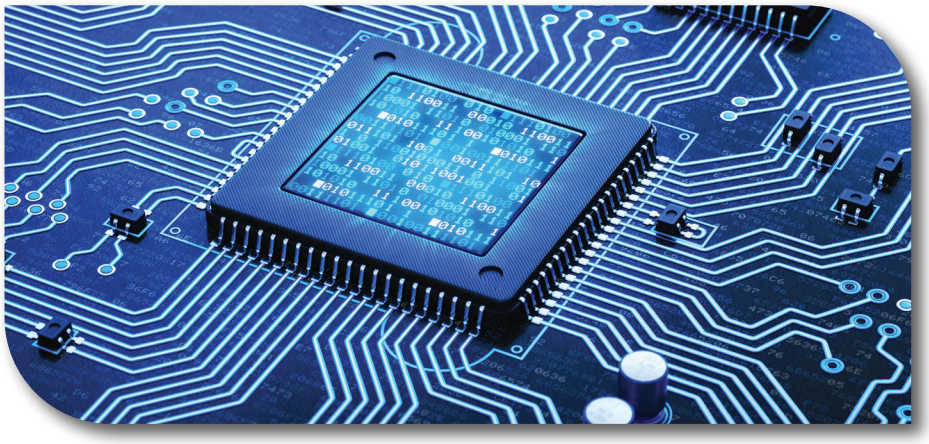
Integrate Technology

- **Technology to Detect**
  - **Sense It.** With increasing sophistication, houses of worship can develop sensor architectures to detect potential threats.

- **Cameras to Sense and Inform.** For example, the integration of camera technology is increasingly cost-effective and extremely advantageous. Cameras are no longer passive detection systems that are realistically just a forensic tool to solve a crime. Today, at increasingly low costs, a camera architecture can be used to inform decisions that prevent intrusion, detect anomalies, and inform action.

- **Technology to Deter**
  - Deterrence of course starts with a mindset that is grounded in sound security practices and reinforced by training. Deterrence is enhanced by technologies that improve access controls and perimeter security.
  - In a recent case study overseas, the mere presence of a walk-through metal detector deterred an attacker set on detonating a suicide vest from entering a house of worship. The mere presence of cameras and access controls that include walk-through metal detectors and basic fencing all complicate a potential attacker's plans.

- **Technology to Defend**
  - Houses of worship should deploy a defense in depth. The depth comes from a series of physical and virtual perimeters, security measures, and technologies.
  - For example, automated lock-down procedures are an increasingly viable option for many houses of worship. With the press of a single button, the ability of an attacker to move unimpeded through a facility can be dramatically reduced. It adds a series of obstacles, increasing the chance to put distance and angles between you and a potential attacker.

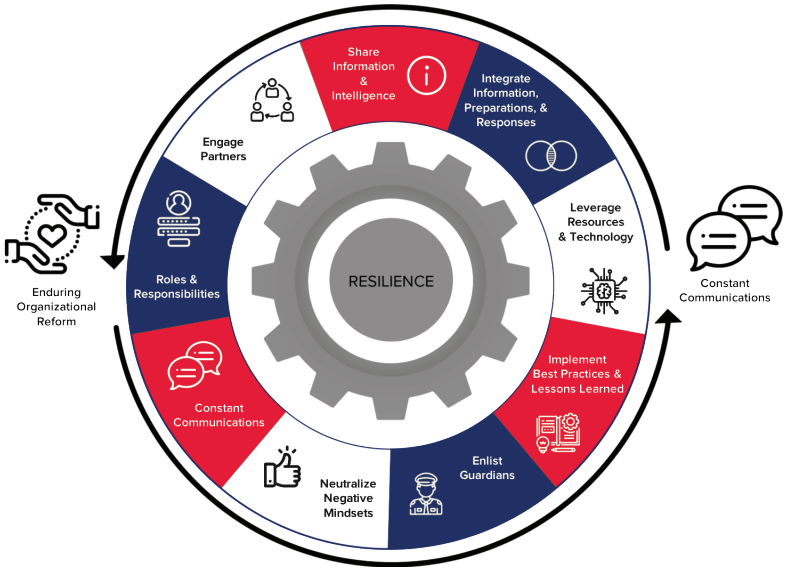


- **Technology to Communicate**
  - One need not look any further than the ubiquitous deployment of smartphones across many congregations. The multiple communication modes from voice to data empower a technological revolution. The ability to communicate with speed and accuracy is dramatically enhanced. A simple email list facilitates routine parish updates, and in crisis, can rapidly inform the congregation on the situation and what actions should or should not be taken. This is further reinforced with voice and text and is enhanced with applications that improve awareness, facilitate intelligence reporting, and provide geospatial location. Many of these applications are encrypted, providing an added layer of security that is particularly important during crisis.

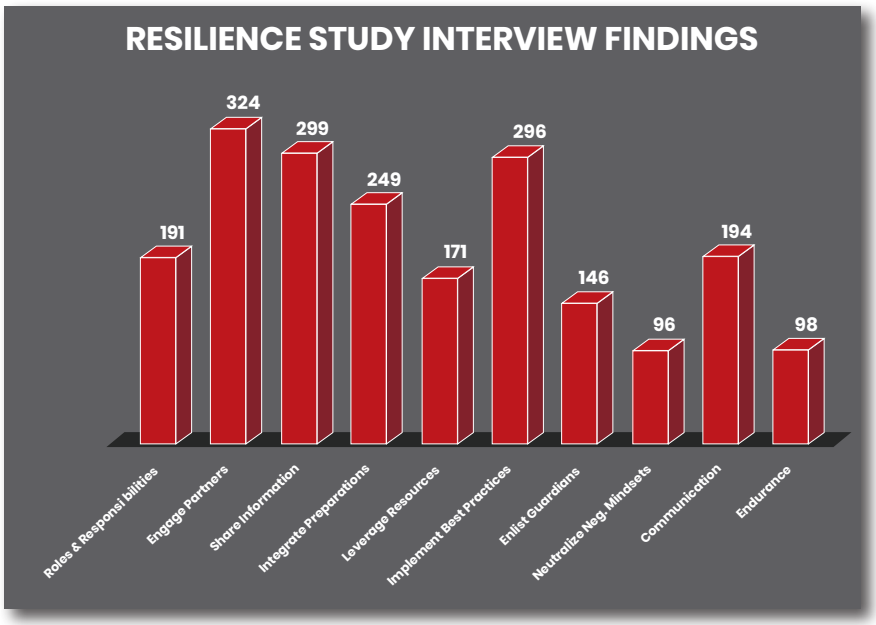
- **Technology at the Speed of Life**
  - The latest generation of sensors are effective, affordable, and able to move at the speed of life —which means security measures operate as fast as the normal movement of the congregation. The deployment of next-generation screening systems can emplace sensors into door frames that passively screen the entire congregation for potentially problematic metal objects at the speed of life. These sensors can detect potential weapons or explosives being introduced into a house of worship and actively cue the security director or usher of an anomaly. In addition, they can also be integrated with camera systems. A passive sensor registers a hit and then cues the focus of the camera system. The system serves as something of a silent and vigilant sentry, always watching and aware. In contrast, security architectures that make already complex and large movements of people harder and slower are difficult to institute and maintain.

Take Action!

- Assess the Current Resource Picture.
- Identify All of the Possible Resource Options Internally and Externally.
- Select the Most Impactful Sources and Actively Pursue these Resources.
- Start Fundraising and Apply for Grants.
- **Integrate Technologies to Detect, Deter, And Defend.**



PRINCIPLE 6: IMPLEMENT BEST PRACTICES AND LESSONS LEARNED



The sixth principle of the RESILIENCE Model is "Implement Best Practices and Lessons Learned," which was noted in the formal interviews more than 290 times. This was the third most discussed pillar collectively by the experts during the interviews. Implementing best practices and lessons learned enhances resilience and reduces the threat to vulnerable communities and houses of worship. Lessons learned can derive from direct or indirect experiences. Direct experiences are security or hazard events that an institution personally encountered. These could range from fire drills to full disaster recovery operations that directly impacted the house of worship. Alternatively, indirect experiences would be the integration of insights from situations that impacted other institutions. Indirect experiences offer houses of worship the opportunity to leverage and implement lessons from other institutions. Partner engagements, the sharing of information, and the review of recent events create an opportunity to learn and adapt to indirect experiences. The key is that a lesson is only learned once implemented.

Only a Lesson Learned Once Implemented

> *Have a plan, rehearse your plan, and then after you've rehearsed your plan, improve your plan.*
>
> *- Kona Zoganas, House of Worship Director of Security*

An enduring pitfall across any organization attempting to prepare for and mitigate hazards is that the execution of training, tabletops, and/or other exercises will end with a thoughtful set of lessons that never get implemented. If the lesson is not implemented, it is not learned, and the institution is not capitalizing on these experiences. After action reports must be done and are critical in capturing key lessons. Once noted, there must be a plan that leads to the implementation of a prioritized list of lessons learned. This plan need not be complex, but rather is often intuitive to its participants and not a significant time burden. The real hazard is that absent the actual implementation of critical lessons learned, the institution will not fully capitalize on security gains despite the significant investment of resources. The following year's exercise may well serve as yet another event that highlights the same gaps and deficiencies, minimizing progress at a time when few institutions have the luxury of excess time or funding.

Lessons Learned Cycle

Overarching attributes of a sustainable and effective lessons learned cycle are rooted in culture. The cultivation of a learning culture that sets high standards, establishes action-forcing mechanisms, and focuses on execution creates an environment where organizational reform and improvement can flourish. The vision of the lessons learned planning and execution cycle is to inspire creativity in solving complex challenges and institute lessons learned and best practices. The goal is to sustain an effective learning and dynamic security posture within a community.

Implementing a Lessons Learned Cycle

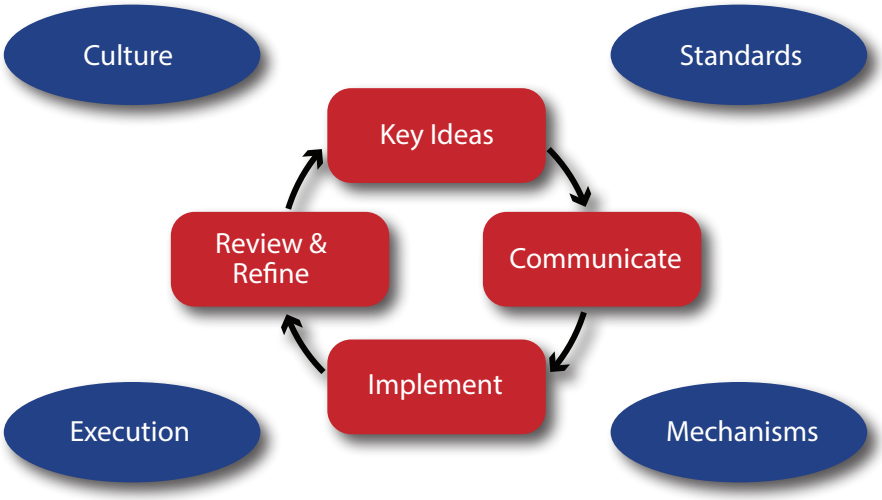
Key Ideas. There are three key ideas or concepts in this section: one is the establishment of a learning culture, the second is the implementation of lessons learned and best practices, and the third is ensuring that this is a continuous process. Establishing a learning culture that systematically implements the lessons and best practices gained from direct experience or from other institutions aids in improvements and adaptations necessary in an evolving threat landscape. Once an institution embarks upon this culture, the next key idea is to focus on actually implementing and integrating lessons learned and best practices continuously. The final key idea is that this is a continuous process of learning and adapting.

Communicate. Communicate, communicate, communicate—this is critical for passing on and codifying key ideas. Learning cultures do not just happen. The cultivation of a learning culture requires leaders who drive its development through constant communications, and it requires the active participation of every member.

Implement. Implementation is essential. The lesson learned, the best practice, or the plan modification all need to be implemented and codified. Institutionalized lessons once learned

drive the change management of the institution, its members, and its governance structure. It prevents the tyranny of personalities or a community stuck in doing things "the way they've always been done."

Review and Refine. The next step in the cycle is the review and refine step. Reviewing the plan or exercise with stakeholders will help identify and highlight deficiencies and gaps. Additionally, the review will identify what went well and what did not. The refinement process addresses the deficiencies by mitigating the gap, applying resources to course-correct, or through reengineering the processes, in order to eliminate the shortfall.

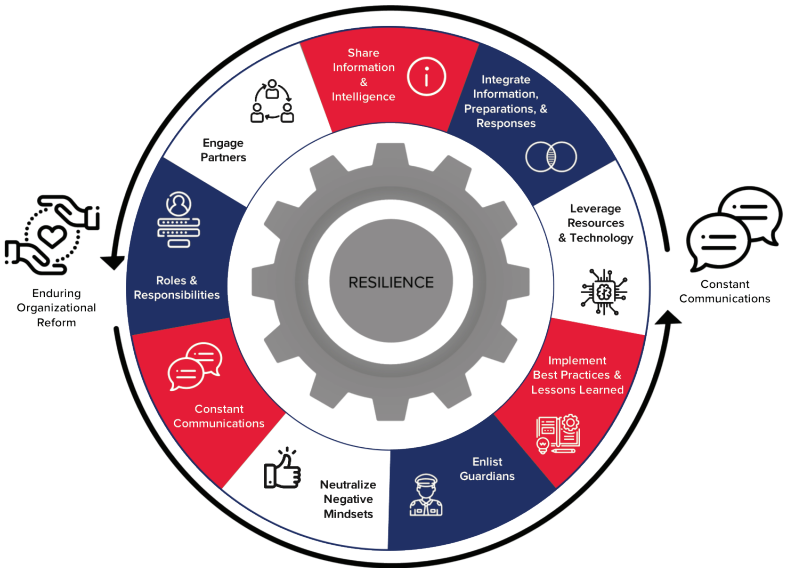


It is important to note that this is a cycle and does not end at refinement. It is imperative that the review of the plan is communicated and changes are highlighted to all stakeholders, partners, and guardians.

Note: This system and cycle can also be used as a strategic guidance process to drive organizational reform. Here, the leader and relevant council establish the big ideas for the institution and then communicate them at every level in a compelling way. Once communicated, there is a natural shift to implementation that requires ongoing communications. As implementation proceeds, there is a routine review and refinement of the key ideas, communications, and implementation. This cycle continues as the organization reforms, adapts, and transforms.

Take Action!

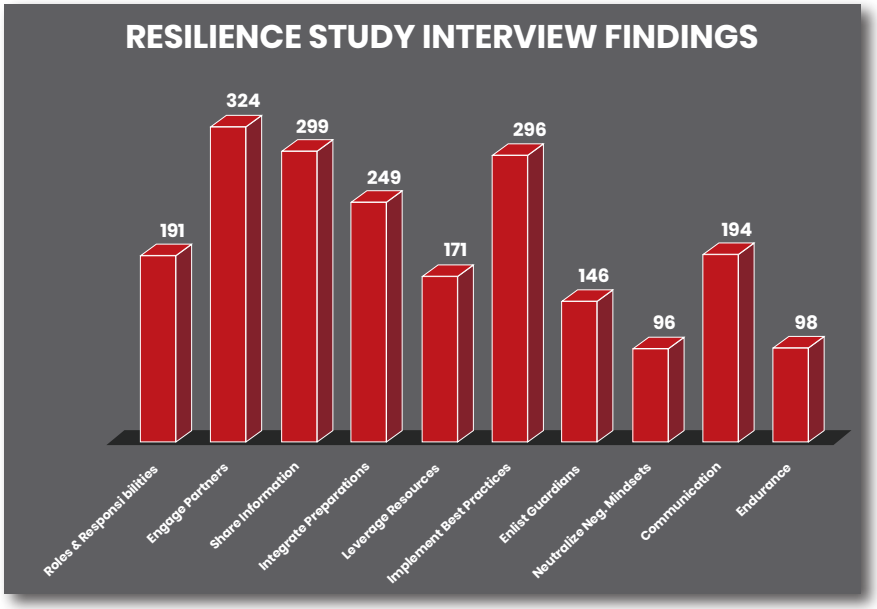
- **Foster a Learning Culture.**
- Pursue Continuous Learning & Implementation.
- Learn, Listen, and Implement from Your Experience.
- Learn, Listen, and Implement from the Experience of Others.
- Remember—Only a Lesson Learned Once Implemented.
- **Implement Best Practices Now.**



PRINCIPLE 7: ENLIST GUARDIANS AND EXECUTE THE PLAN

Guardians for Resilience / Citizen as First Responder

The seventh principle of the RESILIENCE Model is "Enlist Guardians and Execute the Plan." The focus of this principle is for a house of worship to mobilize guardians and execute! Guardians can range from volunteers who serve as ushers welcoming and guiding people into the facility to full-time security staff. Guardians are essential to the execution of plans. Execution or taking action is always the paramount step. According to analysis of the 31 formal interviews, "Enlist Guardians and Execute" unprompted was noted 146 times, as shown in the graph below. The difference between this principle and the second principle, "Engage Partners," is that it focuses on the direct recruitment, development, and deployment of guardians for the execution of safety and security plans rather than the creation of a broad network of critical relationships. The forming of pre-crisis relationships in the second principle is a critical step for enlisting guardians. The second dimension of the principle is focused on execution or taking action. The goal is to put the principles into motion and actually apply the best practices and lessons learned.



> *It helps that our Director of Security was the chief of detectives in Somerset County and ran the county SWAT team.*
>
> *- Robert Lake, Middle School Assistant Principal*

The Importance of Enlisting Guardians

The goal of enlisting guardians is to enhance the preparedness and response of vulnerable communities and houses of worship. They range from internal citizen first responders trained on how to address specific threats, emergencies, and events, to external entities. They include skill sets focused on physical as well as cyber threats.

Internal Guardians

Internal guardians include volunteers and professional staff over whom a house of worship's security leader exercises direct responsibility. Internal guardians are an institution's first line of defense. They are sourced from internal resources and the immediate community. Volunteer guardians are the primary executors of the Citizen as First Responder concept. In the critical minutes before primary first responders arrive to the crisis scene, these volunteer guardians provide initial medical capabilities and evacuation response. Citizens as First Responders may provide initial medical support from CPR to immediate basic trauma care. They enable evacuations during a potential fire and facilitate lockdown procedures during an active shooter event. Volunteer citizens serving as Citizen First Responders are augmented and reinforced where possible by paid professional staff. This team provides a range of support services to include: physical security, cybersecurity, trauma care, and assessment and planning support. It is critical that each institution enlists the unique expertise of its community.

> *"One of the best lines of defense and your first line of defense are your ushers."*
>
> *- Jeff Ringel, Former FBI*

External Guardians

External guardians serve as the next layer of complementary security and expertise that further add depth to the safety and security of a house of worship. External guardians include: the local police agency, fire department, emergency medical, and Federal departments and agencies. House of worship teams do not exercise direct command and control over external guardians. External guardians work with houses of worship, not for them. As the security team engages partners, shares information, and builds plans, houses of worship can develop mutual agreements for various security protocols with external guardians. For example, following a series of credible threats to a house of worship, an agreement is made with local law enforcement to conduct additional patrols and post a police car in front of the primary facility during large public gatherings. These gatherings could be special religious events or community celebrations.

Enlisting the support of external guardians can also include security resources from other houses of worship. An attack against one is an attack against all! To prepare against such an attack, faith communities must organize and cooperate with one another. The more bonds formed between and among faiths, the stronger each community will be.

> *You need to have an established relationship with your **local chief of police, the FBI Joint Terrorism Task Force, the Department of Homeland Security, personnel security, (and) Protective Security Advisor.***
>
> *- Jim Hartnett, Security Director, Secure Community Network*

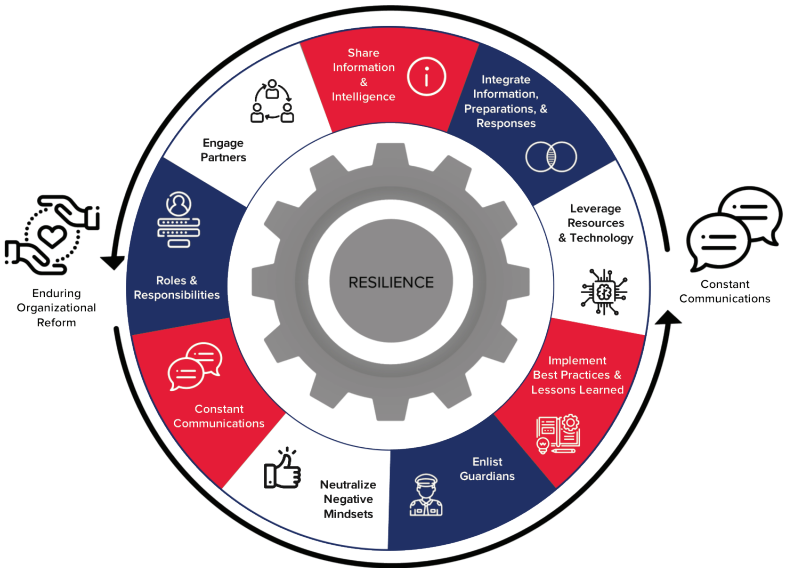
Execute, Take Action

The absolute key to the security and safety of a house of worship is in the execution of the institution's plans, processes, and protocols. To know the RESILIENCE Model in concept is valuable, but the real benefit comes from implementing or executing the model. All too often, institutions assess, but fail to implement. The failure to execute negates the value of an assessment that identifies gaps and recommends security or safety enhancements. Action is always the key, from engaging partners, to sharing information, to executing the response plan. The current threat environment demands action and the timely execution of plans.

> *Institutions should consider hiring security guards to be a deterrent to potential threats and to act as the first responder if an emergency or threatening situation arises.*
>
> *- Paul Goldenberg, Senior Advisor, Rutgers University and Private Sector CEO*

Take Action!

- Enlist Guardians.
- Identify and Deploy Internal Guardians.
- Identify and Deploy External Guardians.
- **Take Action — Execute, Execute, Execute.**

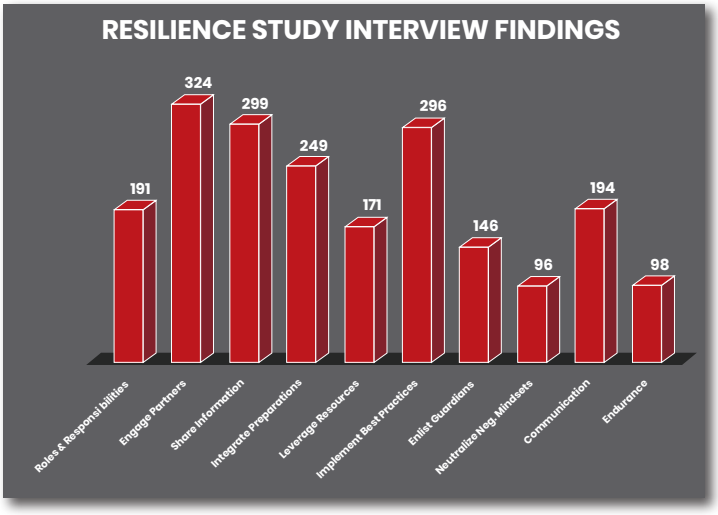


PRINCIPLE 8: NEUTRALIZE NEGATIVE MINDSETS

> *Terrorism and mass violence cannot prevail if people refuse to be terrorized. If people are resilient, if they return to their houses of worship, the assailant fails…*
>
> *– Jeh Johnson, Former Secretary of the U.S. Department of Homeland Security*

The eighth principle of the RESILIENCE Model is "Neutralize Negative Mindsets." The focus of this principle is to ensure an empowering philosophical and psychological paradigm and to reject negative mindsets. The eighth principle in the RESILIENCE Model was referenced 96 times in 31 formal interviews, per the graph below.

Negative mindsets are driven by false premises such as "this will never happen to us," "what can we do about an active shooter?" or "our faith is enough," or "this is inevitable." Negative mindsets degrade preparations and ultimately, response. They curtail a security culture from taking root. Negative mindsets ignore the dangers to a community and disempower individuals. The community can come to believe there is nothing to be done to avoid calamity.



> *Resilience is about mental preparations and how to deal with change.*
>
> *– Bob Liscouski, Former Assistant Secretary, U.S. Department of Homeland Security, Office of Infrastructure Protection*

Mindset and Mental Preparations. Negative mindsets tend to ignore security concerns and underestimate the importance of factoring security considerations into everyday matters. Negative mindsets foster thinking that unfortunate incidents will never happen to one's community or are just inevitable. The right mindset embraces partners and preparations that ensure the safety and security of a house of worship. It believes a catastrophic event is neither inevitable nor completely avertible.

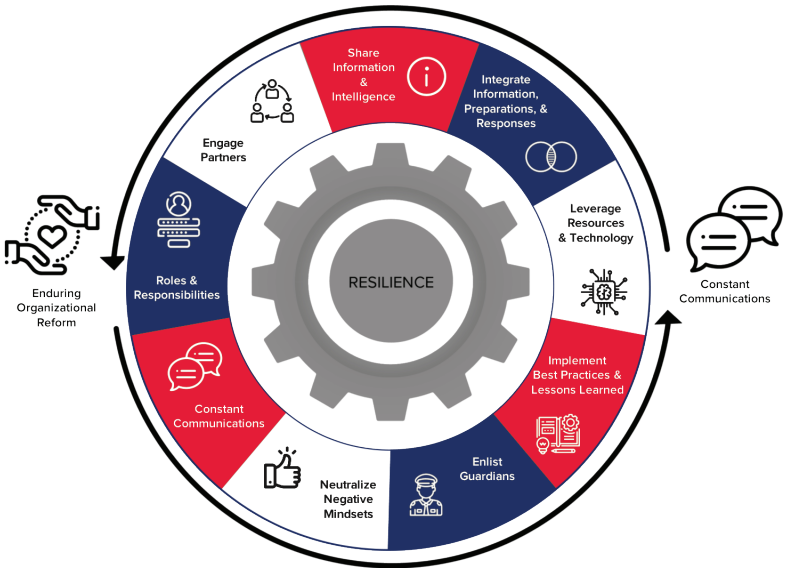
> *When you're talking shootings, you don't want to terrify the kids and make them afraid to go to school. I think if you do it right, the knowledge of what to do will ameliorate the fear that might exist because of the nature of the threat.*
>
> *- John Farmer, Former NJ Attorney General*

Neutralizing Negative Mindsets

- Never Accept the Mindset that an Incident is Inevitable.
- Never Accept the Mindset that an Incident is Completely Avertible.
- Never Accept the Mindset that *"It Won't Happen to Us."*
- Awareness & Preparedness is the Antidote.

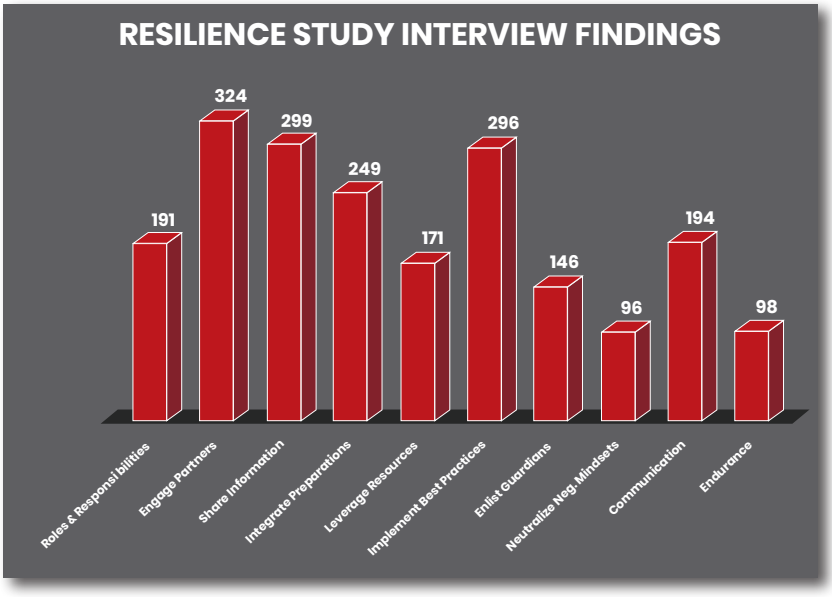
Take Action!

- Accurately Assess the Risk.
- Accept the Reality that Violent Acts can Happen at Any House of Worship.
- Acknowledge the Possibilities.
- Talk About It.
- Ameliorate Fear with Training and Awareness.
- **Do Not Think "If," Think "When" and "What" to Do.**
- **Think "We Can and Will Prepare, Prevent, And Mitigate."**



PRINCIPLE 9: CONSTANT COMMUNICATIONS

The ninth principle of the RESILIENCE Model is "Constant Communications." Houses of worship in constant communication with their partners, guardians, and congregation are better prepared **before, during, and after** an incident. Communications should be routinized and redundant. The strategy should leverage an **all source and method approach**, from traditional face-to-face meetings and calls to social media. Integrated communication plans with partners should be developed. The lead for the execution of the responsibilities of the ninth principle is the Director of Communications. Unprompted, this principle was noted 194 times, as shown in the bar graph below, by every formal interview participant. It is an essential principle in making vulnerable communities better equipped for dealing with criminal activity or ideologically driven violence.



Relationship Between Principles. "Constant Communications" is the key enabling principle within the RESILIENCE Model. It facilitates communications across stakeholders and across the principles of the RESILIENCE Model. For example, it facilitates the sharing of information, the engagement of partners, and the integration of preparations and responses. The third principle, "Sharing Information and Intelligence," focuses on the need to gather, analyze, and share potential threat information. While this ninth principle of "Constant Communications" is the enabler for this, to include the dissemination of information, it is also a central pillar in its own right. The ninth principle focuses on preventing and preparing for incidents through constant communications. It is a key element of principle four, the "Integration of Information, Preparations, and Responses."

Link to the World

"Constant Communications" is the pathway that allows for the sounding of the alarm in crisis. It enables the internal and external roles of partners before, during, and after an incident. Before a disruptive event, constant communications enable the exchange of threat information and best practices. During an incident, "Constant Communications" ensures awareness and a unified response. It allows stakeholders to better understand the situation and what they can do to help.

Before an incident
During an incident
After an incident

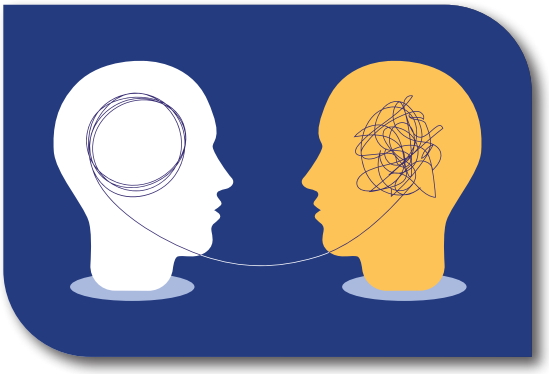
Communicate All the Time
All Source and Method Approach

After an attack, principle nine helps to mitigate false information and narratives. It ensures that the most accurate and reliable information possible is released as soon as possible. It allows all members of the community to understand and it facilitates recovery. "Constant Communications" helps inoculate a community and reduce the chaos brought on by a disruptive event.

Without robust and reliable communications, plans quickly fall apart. Team members become unaware of what tasks should be executed and if their actions are coordinated and complementary. Steps can be overlooked and members may focus on the wrong actions. Imagine multiple agencies and departments responding to a crisis, but no one is talking to each other or saying what they are doing. This of course sounds like a recipe for chaos, and all too often, it is a reality. "Constant Communication" is vital for coordination and a unified response.

As shown in the resilience wheel diagram, "Constant Communications" is key in building resilience in houses of worship. It is its own separate portion of the model's resilience wheel and is an aspect of RESILIENCE that is carried throughout the other nine principles. It ensures the communication of crisis plans, and that every stakeholder understands what is going on, whether through engaging partners (principle two) or through implementing best practices (principle six).

Internal vs. External Communications



There are two primary communication pathways when working in teams before, during, and after an act of man or nature. The two pathways are internal and external communications.

Internal communications focus within the house of worship. This includes leadership, internal security and safety teams, and the faith community. It often times can be thought of as communications among those most immediately impacted by an event. Here, all forms of communication occur within a house of worship and its members. This can be done through face-to-face gatherings, social media, or direct religious events.

> *"This business of emergency response is all about relationships and being able to communicate, first and foremost..."*
>
> *- Kona Zoganas, House of Worship Director of Security*

External communications are focused on partners like first responders, local, state, and Federal departments, the media, and the general public. Constant external communications prior to an event ensure readiness. During an event, it enables a coordinated response. It optimizes the promulgation of critical information in the most chaotic of times and will help the media get the right story the first time. This type of communication consists of all mediums from in-person to web-based content.

Communicate, Communicate, Communicate. The key to building resilience in houses of worship is to talk constantly to all partners and guardians. When communities communicate, they become more prepared, resilient, and ready!

Develop a Communications Plan

Speaking with one voice before, during, and after crisis is essential. In this day and age, to not have a communications plan is tantamount to accepting chaos in crisis. With principle one, houses of worship identify and fill the role of the Communications Director who is the lead for developing the steady state and crisis communications plan. The communications plan need not be overly complex. It will address key basics that include: Who is communicating? What are they communicating? When? Why? The plan will routinize communication channels internally and externally. Such standardization increases the flow of accurate information. At the point of crisis, it enables more agile responses, improves coordination, and reduces friction. During a crisis, errant communications, everyone or no one talking, and the dissemination of false information will increase uncertainty. Increased uncertainty compounds the invariable chaos of the event, which further degrades the response.

> *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, Former NJ Attorney General*

The following guidance should be considered in a communications plan or strategy:

- Communications will be timely and honest.
- To the extent possible, staff and the congregation should hear news from the Director of Communications or the head of the congregation first.
- Communications will provide objective and subjective assessments.
- All staff should be informed at approximately the same time (when possible).
- Give bad news all at once – do not sugarcoat the truth.
- Provide the opportunity to ask questions (if possible).
- Provide regular updates and let people know when the next update will be issued.
- Communicate in a manner appropriate to circumstances:
    - Face-to-face meetings (individual and group)
    - News conferences
    - Social media
    - Voicemail/email
    - Intranet and internet sites
    - Toll-free hotline
    - Special newsletter
    - Announcements using local/national media

Steady State Communications Plans. Create a steady state communications plan that allows all stakeholders to communicate on a regular basis. This plan is for day-to-day operations. It can consist of daily, biweekly, or weekly phone calls. It can include in-person engagements, emails, or social media content. The intent of the steady state plan is to routinize communications that improve day-to-day operations and build the pathways between people before crisis knocks.

Crisis Communications Plan. The crisis communications plan builds off the steady state plan. Think of it as the next layer of the communications plan. The key difference is the context and the need for speed. The context is an event like an active shooter or a mass casualty event that triggers the initiation of all crisis plans and actions.

The activities that declaring a crisis will trigger include, but are not limited to:

- Additional call notification
- Evacuation, shelter, or relocation
- Safety protocol
- Response site and alternate site activation
- Team deployment
- Personnel assignments and accessibility
- Emergency contract activation
- Operational changes

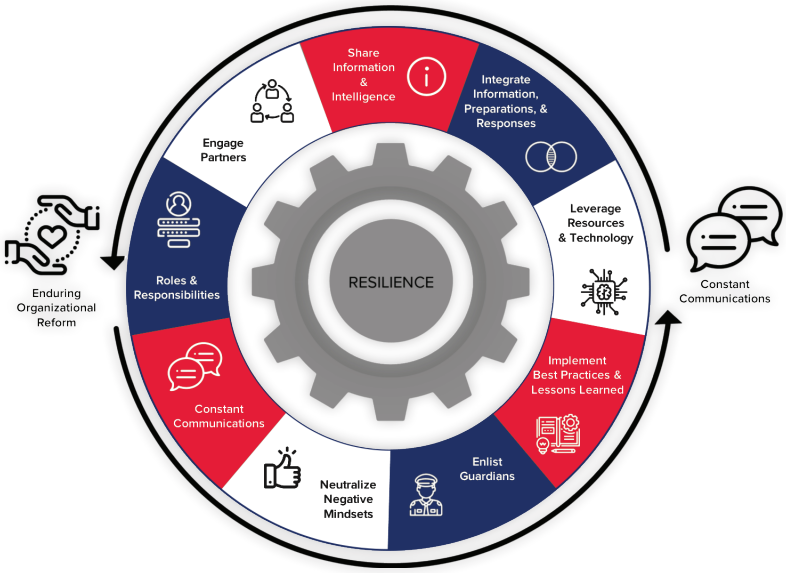
Redundancy Equals Reliability and Readiness

The Director of Communications is the primary for the ninth principle. However, the Director of Communications should have a back-up person and/or team. In the event that the lead for communications is on travel or caught in the actual incident, an alternate and tertiary Communications Director should be identified. The alternate and tertiary directors should be fully trained and ready to engage. Collectively, the communications team, be they staff or volunteers, develops the communication protocols and tools and offers guidance that clarifies what should be communicated, when, and by whom. The team also identifies what should not be communicated in times of crisis. The communications protocols also identify available communication tools, channels, and partners. Beyond the communications team, it is critical that all stakeholders are aware of the tools and channels available for communications. These pathways enable the security team and the congregation to maintain an enhanced situational awareness. Building redundancy within the communications personnel, plans, and pathways is integral to the safety, security, and resilience of a house of worship. Leverage steady state communication actions as the building blocks for the passing of critical information in crisis. The pathways used to communicate every day with partners, staff, and the congregation can serve as practice sessions for crisis. In crisis, time will invariably be compressed, while pressure is increased and the need to get it right will be a premium. The repetitions gained through daily communications maximize the probability of success at the point of crisis. The development of completely independent crisis protocols should be minimized.

> *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 backup 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, Security Director, Secure Community Network*

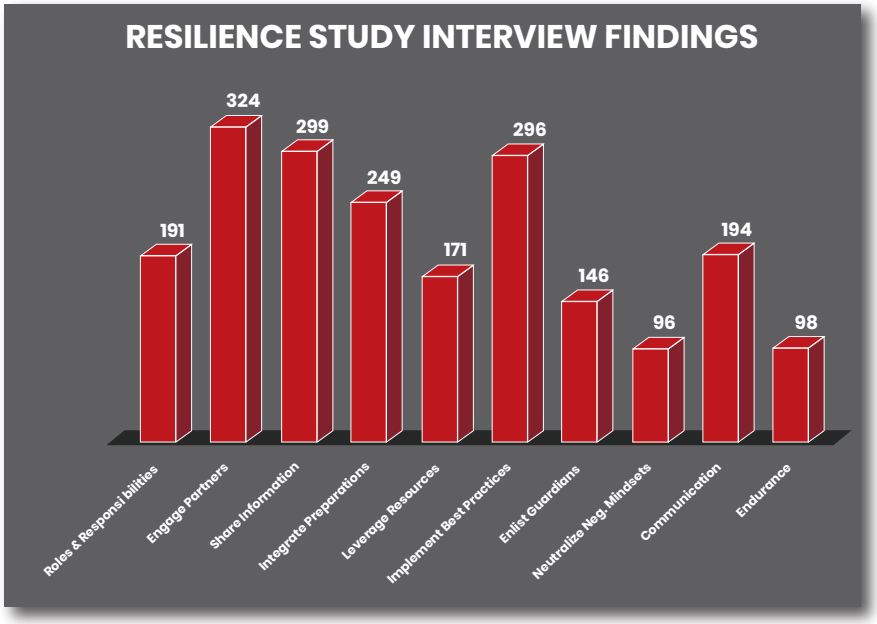
Take Action!

- **Communicate Constantly!**
- Build a Steady State (Non-Crisis) Plan and Execute.
- Build a Crisis Plan.
- All Source Approach (From Calls to Social Media).



PRINCIPLE 10: ENDURING ORGANIZATIONAL REFORMS AND READINESS

The tenth principle of the RESILIENCE Model is "Enduring Organizational Reforms and Readiness." This final principle of the model is focused on the need to codify and institutionalize safety and security practices to ensure lasting reforms and readiness. It is the final step to empowerment. This is a long game against an unpredictable adversary. Houses of worship must prepare today and sustain those preparations into perpetuity. Reforms must be institutionalized. Readiness is not a one-time thing. Although only mentioned 98 times during interviews, enduring reforms and readiness are a major component in ensuring the success and longevity of an institution.



> *You develop resources and institutions that are necessary for creating awareness, creating empowerment, and reassuring the community that their voice can be heard.*
>
> *– Ali Chaudry, NJ Interfaith Advisory Council Member*

Enduring Reforms—Institution Building. Houses of worship must institutionalize their success to ensure that lessons learned are documented and implemented. No institution can afford not to learn lessons from training, exercises, or crisis multiple times. To make reforms enduring, houses of worship must develop standing operational procedures. Codify plans, procedures, people, and protocols to lock in the best insights. Security teams must avoid the following perils: no documentation, no dissemination, no follow-up, no institutionalization of reforms. Creating the necessary institutions and structures is critical.

Enduring Readiness and Institutional Vigilance. The current threat picture is increasingly disruptive and unpredictable. Time, place, location, and target selection are at times carefully selected and in other cases, completely random. At times, houses of worship are preparing for a once-in-a-generation catastrophic attack. Simultaneously, they are managing day-to-day challenges ranging from the provision of strained services to the countering of criminal activities. Services, safety, funding, crime, cyber, and infrastructure maintenance all create a busy and chaotic environment for the head of a congregation and the Director of Security. Readiness must be a constant priority. To ensure readiness, the systematic codification of institutional reforms is essential. The need to be constantly vigilant and integrate endurance into plans and posture is essential for resilience.

Avoid the Peril of Peek Activity Followed by Protracted Inactivity. Rare, brief, violent, and chaotic events generate peek activity and hyper-vigilance. Often times it is a level of activity and vigilance that simply cannot be maintained. The institutional endurance necessary for this level of heightened activity often times does not exist. Hyper-vigilance is frequently quickly followed by dramatic drops in security protocols. Endurance is also about pacing. This is not a sprint, but rather a marathon. It is a journey that requires enduring organizational readiness. Avoiding the perils of peek activity followed by protracted inactivity mitigates gaps in security and awareness. The tenth principle ensures continuity and vigilance.

Take Action!

- Build Enduring Organizational Reforms.
- Be Ready, Every Day.
- Create a Sustainable Awareness and Security Posture.

CONCLUSION

The research findings and attack statistics indicate a significant rise in threats to houses of worship and vulnerable communities. While longer lead policy efforts at the national level attempt to curb this rise in violence, houses of worship need to take prudent measures to ensure the security and safety of their respective communities. The RESILIENCE Model offers an evidence-based system that can, with minimal resources, enhance the security of houses of worship and vulnerable communities. Its ten principles, grounded in evidence and experience, offer a series of lighthouses that can move a community toward safer waters. The principles serve as guideposts and the corresponding material a path for execution. Further, this report can serve as a standalone guide or it can integrate and be complemented by a broad range of well-produced security reports, manuals, and checklists. Examples of such works are included at the end of this report in Appendix B.

The RESILIENCE Model can be put into action through a linear execution from the first to the tenth principle. Here the journey starts with the first principle, which focuses on roles and responsibilities, then partners, and on through the next eight principles. Admittedly, the sequencing of the principles is intended to have a logical order where one builds upon the next. Arguably, the RESILIENCE Model is most impactful when the system is executed in this order. However, putting the RESILIENCE Model into action need not be a lockstep process. The principles can be executed in alternate sequences based on priorities, gaps in existing security efforts, and the availability of internal or external resources. Whether the plan of action is linear or prioritized based on unique challenges and opportunities, the key is to take action. Start putting the evidence-based principles of the RESILIENCE Model to work today. Cumulatively, the RESILIENCE Model principles enable a strategic path to a resilient community.

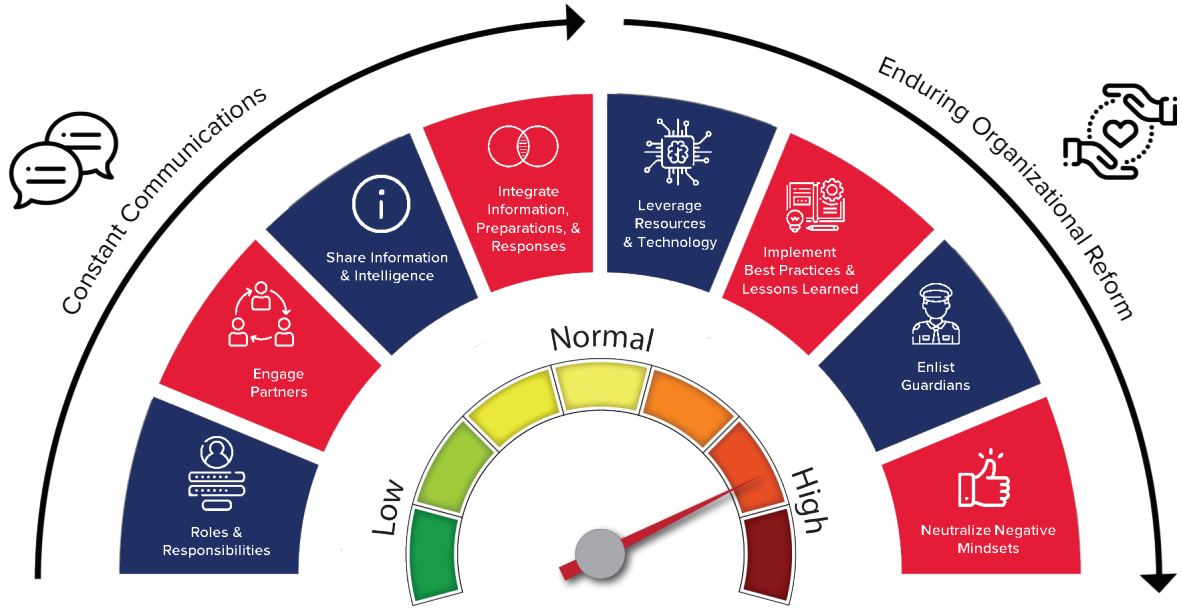
R.E.S.I.L.I.E.N.C.E. Model Principles

1. Roles and Responsibilities
2. Engage Partners
3. Share Information and Intelligence
4. Integrate Information, Preparations, and Responses
5. Leverage Resources and Technology
6. Implement Best Practices and Lessons Learned
7. Enlist Guardians and Execute the Plan
8. Neutralize Negative Mindsets
9. Constant Communications
10. Enduring Organizational Reform

ACKNOWLEDGEMENTS

First and foremost, Dr. Clark extends his great thanks to all of the report's interview participants who universally contributed profoundly to the evidence base. The interview participants generously gave their time, passed on true wisdom, and actively supported finding the next cohort of interview participants for the study. To the Rutgers family, deep thanks to John Farmer, the Director of the Eagleton Institute. John's enduring support and experience made all the difference. Thanks as well to the broader Rutgers family, Ava Majlesi, Director of the Critical Intelligence Studies Program, and for the opportunity to mentor and inspire a group of young fellows for public service to include: Christina Gaudino, Gavin Mayes, Christopher Lugo, Teresa Ngo, Dawn Park, and Kristen Raushenberger. Deep thanks to Matt Molinari, who was essential to the interview process and now serves as an Ensign in the United States Navy deployed overseas. With special thanks to Jeh Johnson, Russ Deyo, and Shannon Kula for their enduring friendship and insights. Jeh Johnson and Russ Deyo are dear friends and profound sources of inspiration. Their support and wisdom have made all the difference. Finally, to Dr. Shannon Kula who I could never thank enough for her intellect and profound contributions to this study.

APPENDIX A.1 RAPID RESILIENCE ASSESSMENT



Guidance:

10 Resilience Model Principles each valued at 0 to 10 Points.
Rapid Assessment 10x10 = 100.
Total Valuation from 0 to 100.

Principle	Value	Score
1. Roles & Responsibilities	0 -10	
2. Engage Partners	0 -10	
3. Share Information & Intelligence	0 -10	
4. Integrate Information, Preparations & Responses	0 -10	
5. Leverage Resources & Technology	0 -10	
6. Implement Best Practices & Lessons Learned	0 -10	
7. Enlist Guardians & Execute	0 -10	
8. Neutralize Negative Mindsets	0 -10	
9. Constant Communications	0 -10	
10. Enduring Organizational Reform	0 -10	
Total Score:	0 -100	

APPENDIX A.2 DELIBERATE RESILIENCE ASSESSMENT

Guidance:

10 Resilience Model Principles.
Deliberate Assessment Total Valuation 0 to 100.
Principles 1, 2, 3, 5, 6, 7, 9 valued from 0 to 10.
Principle 4 valued from 0-20 and principles 8 and 10 valued from 0-5.

Principle	Value	Score
1. Roles & Responsibilities Roles Identified (2 points) Responsibilities Identified (2 points) People Identified and Designated (2 points) People Ready to Perform Designated Roles & Responsibilities (4 points)	**0-10** **2** **2** **2** **4**	
Principle 1 Sub Score		
2. Engage Partners Congregation (2 points) Local Community (2 points) Law Enforcement (Local, State, Federal) (2 points) Fire Department and Emergency Medical (2 points) National Organizations, Associations (2 points)	**0-10** **2** **2** **2** **2** **2**	
Principle 2 Sub Score		
3. Share Information & Intelligence (GAS) Gather (4 points) Analyze (2 points) Share... With Congregation and Local Community (2 points) With First Responders and Other Partners (2 points)	**0-10** **4** **2** **2** **2**	
Principle 3 Sub Score		
4. Integrate Information, Preparations & Responses Preparations (Assess: 3 points, Plan: 3 points, Train & Exercise: 4 points) Responses (Before: 4 points, During: 3 points, After: 3 points)	**0-20** **10** **10**	
Principle 4 Sub Score		
5. Leverage Resources & Technology Resources, Public and Private (6 points) Technology (4 points)	**0-10** **6** **4**	
Principle 5 Sub Score		

Principle	Value	Score
6. Implement Best Practices & Lessons Learned Continuous Assessment (5 points) Implementation (5 points)	**0–10** **5** **5**	
Principle 6 Sub Score		
7. Enlist Guardians & Execute Enlist Internal and External Guardians (5 points) Internal: Citizen as First Responder External: First Responders, Funders and Planners Execute, Take Action (5 points)	**0–10** **5** **5**	
Principle 7 Sub Score		
8. Neutralize Negative Mindsets Never Accept the Mindset that an Incident is Inevitable (5 points)	**0–5** **5**	
Principle 8 Sub Score		
9. Constant Communications Steady State (Non-Crisis) Plan and Execution in Place (5 points) Crisis Plan in Place (3 points) All Method and Source Approach (From Calls to Social Media) (2 points)	**0–10** **5** **3** **2**	
Principle 9 Sub Score		
10. Enduring Organizational Reform Institutionalizing Organizations, Actions, and Reforms (5 points)	**0–5** **5**	
Principle 10 Sub Score		
Total Score:	**0–100**	

R.E.S.I.L.I.E.N.C.E. Model Principles

1. Roles and Responsibilities
2. Engage Partners
3. Share Information and Intelligence
4. Integrate Information, Preparations, and Responses
5. Leverage Resources and Technology
6. Implement Best Practices and Lessons Learned
7. Enlist Guardians and Execute the Plan
8. Neutralize Negative Mindsets
9. Constant Communications
10. Enduring Organizational Reform

APPENDIX B. EXAMPLE RESOURCES FOR HOUSES OF WORSHIP AND FAITH-BASED COMMUNITIES

Department of Homeland Security (DHS)

- **DHS Ready.gov**
  https://www.ready.gov/
- **"If You See Something, Say Something" Campaign**
  https://www.dhs.gov/see-something-say-something
- **DHS Active Shooter Preparedness**
  https://www.dhs.gov/active-shooter-preparedness
- **Protective Security Advisors, DHS Infrastructure Protection**
  http://www.dhs.gov/files/programs/gc_1265310793722.shtm
- **National Cybersecurity and Communications Integration Center**
  https://www.us-cert.gov/nccic
- **Homeland Security Information Network (HSIN)**
  http://www.dhs.gov/files/programs/gc_1156888108137.shtm
  Note: Contact HSINCS@dhs.gov to obtain a username and a password that will allow access to several tools, including a webinar entitled "The Evolving Threat: What You Can Do."
- **SAR Training for Hometown Security Partners**
  https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training
- **Nationwide SAR Initiative (NSI) Resources**
  https://www.dhs.gov/nationwide-sar-initiative-nsi/nsi-resources
- **DHS Center for Faith-Based and Neighborhood Partnerships**
  https://www.dhs.gov/dhs-center-faith-based-neighborhood-partnerships
- **DHS Office for Bombing Prevention Training and Resources**
  https://www.cisa.gov/office-bombing-prevention-obp
- **DHS Community Engagement, Outreach, and Training Resources**
  http://www.dhs.gov/community-outreach-and-training
- **Community Preparation Through the Hometown Security Program**
  https://www.dhs.gov/hometown-security
- **DHS Office for Civil Rights and Civil Liberties, Community Engagement Section**
  http://www.dhs.gov/crcl
- **Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Safety for Faith-Based Events and Houses of Worship (April 2017)**
  https://www.dhs.gov/sites/default/files/publications/17_0531_NSI_SAR-Faith-Based-Events-Houses-Worship.pdf
- **Guide for Developing High-Quality Emergency Operations Plans for Houses of Worship**
  https://www.dhs.gov/sites/default/files/publications/Developing_EOPs_for_Houses_of_Worship_FINAL.PDF
- **DHS Houses of Worship Security Practices Guide**
  https://www.illinois.gov/ready/plan/Documents/DHS_Houses_of_Worship_Security_Practices_Guide.pdf

Federal Emergency Management Agency (FEMA)

- **Resources to Protect Your House of Worship**
  https://www.fema.gov/faith-resources
- **FEMA Management Institute Training Resources**
  http://www.training.fema.gov/EMI
- **FEMA Guide for All-Hazards Emergency Operations Planning**
  http://www.fema.gov/pdf/plan/slg101.pdf
- **Comprehensive Preparedness Guide 101**
  https://www.fema.gov/media-library-data/1573581112287-035972e4d26817854c833457863c34cc/201911Listening_CPG_101_V2_22NOV2010.pdf

Department of Justice and FBI

- **U.S. Department of Justice Community Relations Service**
  http://www.justice.gov/crs/index.html
- **FBI Resources for Law Enforcement, Businesses, and Victim Assistance**
  https://www.fbi.gov/resources
- **FBI Information on Hate Crimes**
  https://www.fbi.gov/investigate/civil-rights/hate-crimes
- **Protecting Houses of Worship Event Resource Guide, U.S. Attorney's Office, District of CO (Download)**
  https://www.hsdl.org/?view&did=790107
- **Justice Technology Information Center: Safeguarding Houses of Worship**
  https://www.justnet.org/resources/Houses_of_Worship.html

The National Counterterrorism Center (NCTC)

- **NCTC's "Homegrown Violent Extremist Mobilization Indicators for Public Safety Personnel"**
  https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/item/1945-homegrown-violentextremist-mobilization-indicators-2019

Resources from Faith-Based Organizations and Interfaith Organizations

- **Secure Community Network**
  https://scnus.org/institutional-security
- **Christian Emergency Network**
  http://www.christianemergencynetwork.org/
- **National Disaster Interfaith Network**
  http://www.n-din.org/
- **Active Shooter in a House of Worship**
  http://www.n-din.org/ndin_resources/tipsheets_v1208/07_NDIN_TS_ActiveShooter.pdf

Resources from Private Sector Companies and Non-Governmental Organizations

- **ASIS Recommended Best Practices for Securing Houses of Worship**
  https://www.asisonline.org/About-ASIS/Documents/SecuringHOWs.pdf
  Note: to access this resource, you will need to sign in or create an account.
- **ASIS International**
  https://www.asisonline.org/publications--resources/security-topics/securing-houses-of-worship/
- **Information Sharing and Analysis Organizations (ISAO)**
  https://www.isao.org/about/
- **Faith-Based Information Sharing and Analysis Organization (FB-ISAO)**
  https://faithbased-isao.org/about/
- **Information Sharing and Analysis Centers (ISAC)**
  https://www.nationalisacs.org/