**Fixing Roofs and Planting Trees**

It has been said that the best time to plant a tree was 30 years ago, and the second-best time is now. More recently, FBI Director Christopher Wray commented "The best time to fix a leaky roof is when the sun is shining."

These quotes highlight the importance of not waiting for a crisis to occur to start planning for it.

With the increase in incidents of targeted violence across the United States, having a security plan for your institution is essential. Proper planning helps organizations manage risk and increase resiliency. Imagine the impact (physical, financial, emotional) of a fire, natural disaster, or terrorist attack at your facility. Having even a basic plan for how your organization will react to such an event will help reduce the physical, emotional, financial, and other associated impacts.

While the idea of security and emergency planning can be intimidating and overwhelming, it is not as complicated as it seems. By forming a security committee, and breaking the process down into a few key elements, it becomes less daunting, and you can readily develop a plan that will help keep your organization safe.

Forming a security committee allows for the distribution of the workload and assures that subject matter expertise is available across a variety of disciplines. The composition of the committee should include not only those responsible for security, but also maintenance personnel, board members, clergy, administrators, teachers, local first responders, and any other entity with a stake in the outcome. Building important relationships with first responders and other community stakeholders takes nothing but a little time, effort, and maybe the price of a cup of coffee.

During the January 15, 2022, hostage standoff at Congregation Beth Israel in Colleyville, TX, hostage Rabbi Charlie Citron-Walker exchanged text messages with Colleyville police chief Michael Miller, providing critical intelligence needed by law enforcement responders outside. This would not have been possible without the existing relationship between Rabbi Charlie and Chief Miller, which was established "when the sun was shining," well before the crisis. Rabbi Citron-Walker's established relationships with area faith leaders within and outside the Jewish community were of value as the congregation recovered and reestablished its important role in the community. Although it took three months to repair and reopen Temple Beth Israel, the congregation resumed services at a nearby church the week after the attack.

Rabbi Citron-Walker also credited the training programs offered by various organizations that he and other members of the congregation attended with enabling him to remain calm and take decisive action that ultimately saved his own life and that of the other hostages.

Once you've formed your committee, the first action to be taken should be to conduct a risk assessment. A risk assessment establishes a baseline of threats (external, such as weather, fire,

crime, terrorism, etc.) and vulnerabilities (internal, such as poor access control, defective doors or windows, poor lighting, lack of policies, etc.) specific to your organization, which ensures that your subsequent planning efforts are appropriately focused.

An example of the risk assessment process would be the Terrorism Risk and Vulnerability Assessments that CSI performs free of charge for organizations that wish to identify terrorism-related threats and vulnerabilities. The report generated by this process provides a roadmap of action steps to reduce vulnerabilities and can be used to support applications for state and federal security grant programs. The ultimate goal of this first step is to identify mitigation actions that can help reduce the likelihood of an incident, and should an incident occur, reduce the impact of that incident. In addition to CSI, private security consultants can conduct such assessments for a fee, and there are several tools available online to assist organizations in conducting their own self-assessments.

Once the assessment has been completed, it should be used to guide the process of planning, and of mitigating vulnerabilities. The essential components of a facility security plan include:

- Written policies and procedures: These should include, but not be limited to access control processes, opening and closing routines for your building at the beginning and end of the day, decision-making, and internal and external communication.

- Physical security measures: A well-designed physical security system that is appropriate for your facility is an important part of a security plan. Physical security systems include items like security-rated doors, locks, windows, cameras, alarms, access control systems, fences, vehicle barriers, and so forth. Not all physical security systems include all the listed equipment; the system should be tailored to your organization's specific needs.

- Emergency response plans: Outline specific actions to take during an emergency such as an active attack, bomb threat, or other hazard. Emergency response plans should also address the recovery phase after the incident, to ensure the organization addresses continuity of operations, repairs to physical damage, and healing the emotional trauma that accompanies a disaster.

- Training and exercises: Once the plan is disseminated to all concerned, training should be conducted to ensure that anyone responsible for executing all or parts of the plan is familiar with the plan and can perform the tasks specified in the plan. Exercises should be conducted to simulate an actual emergency to reinforce training and identify improvement areas.

- Periodic review: Plans should be reviewed and updated regularly to ensure that they are still appropriate in their current form. At a minimum, plans should be reviewed after an incident, following an exercise, after a change in leadership or other key personnel, changes or improvements to the facility or its security measures, and changes to the threat environment.

Security planning is a steady-state activity with no endpoint. Like a tree, it is constantly evolving iteratively, forming new branches and growing in different directions as needed to adapt to changing threats, vulnerabilities, and risks.

Don’t wait for a security crisis to start thinking about how your organization will handle such an event; by then it’s too late. Plant your metaphorical trees and fix your metaphorical roof now to ensure your organization is well-prepared for such an eventuality.