




减少宗教场所袭击

安全指南

2020 年 12 月



**要减少可能的
袭击,最好的
办法就是采取
整体安全方法。**

目录

Assistant Director 来信.....	1
大纲.....	2
介绍：保护宗教场所.....	4
宗教场所在美国社会中的独特角色.....	4
宗教场所袭击.....	5
Department of Homeland Security 的使命是什么？.....	5
CISA 的工作是什么？.....	6
指南概述.....	6
1 了解问题.....	9
介绍.....	9
查询文献和全国的趋势.....	10
制定案件研究的方法.....	14
针对性暴力.....	15
案件研究中纳入的操作定义.....	15
事件案件研究.....	16
事件概述.....	16
纵火和爆炸.....	17
网络攻击.....	20
武装袭击和大规模枪击.....	20
袭击后果.....	21
犯罪者.....	21
目标宗教场所.....	23
犯罪者的战术和方式.....	24
之前关联.....	24
纵火和爆炸.....	24
行为迹象.....	24
武装袭击.....	25
网络攻击.....	26
安全实践.....	28
总结.....	28

2	制定整体安全方法	31
	介绍	31
	什么是整体安全方法?如何实现这一方法?	31
	关键概念、术语和问题	32
	制订整体安全策略的框架	35
	入门: 设立岗位和职责	35
	规划流程	36
	整体安全策略的构件: 如何保障宗教场所的安全	36
	总结: 出台整体安全策略	37
3	开展全面薄弱环节评估	39
	介绍	39
	分配岗位和职责	39
	确定薄弱环节评估的范围	40
	薄弱环节评估模型	41
	运用薄弱环节评估模型的主要考虑事项	42
	组织的资产	42
	进行原样审核	43
	全面威胁分析	44
	确定与风险有关的成本和后果	45
	确定风险解决方案并排定缓解措施优先级	46
	总结	46
4	做好社区准备和防范	49
	介绍	49
	您 HoW 社区的最佳实践	49
	建立安全文化	50
	认知和尽早识别	50
	If You See Something, Say Something®	51
	问候的力量	52
	跑开、躲藏、反击	53
	心理健康和社会支持服务	54
	特殊政策和长期规划	55
	应急规划和事件响应	55
	人员安全实践	56
	内部人员威胁	56
	报告程序	57
	更大范围的社区参与	58
	事件规划	58
	社区参与	59
	战略合作关系	60
	总结	61

5	保护您的设施	63
	介绍	63
	外部边界	64
	建筑中间	66
	建筑内部	68
	总结	70
6	托儿所和学校安全注意事项	73
	介绍	73
	设施评估	73
	程序和规定	74
	物理安全	75
	学校氛围	75
	行为健康	76
	培训	77
	资助资源	78
	总结	78
7	网络安全	81
	介绍	81
	网络袭击类型	81
	金融欺诈	81
	勒索软件	82
	网站篡改	82
	建立网络攻击应对准备文化	82
	网络清洁环境	83
	在线安全	84
	安全实践和认知	85
	瓦解具体的威胁	87
	恶意软件和病毒	87
	网络钓鱼攻击	87
	勒索软件	88
	网站篡改	88
	总结	89
8	总结和总体结论	90
	展望	91

附录 1: 宗教场所综合资源 93

第 1 章: 介绍	93
第 2 章: 确定整体安全方法	93
应急准备	93
应急操作	94
业务连续性	94
第 3 章: 开展全面薄弱环节评估	94
第 4 章: 做好社区准备和防范	95
威胁管理	95
社区参与和社区关系	95
专业联络伙伴关系	96
心理健康和社会支持服务	96
第 5 章: 保护您的设施	96
拨款	96
用设计求安全	96
威胁管理	96
第 6 章: 托儿所和学校安全注意事项	97
一般资源	97
物理安全	97
学校氛围	97
培训	97
资助资源	98
第 7 章: 网络安全	98
网络清洁环境	98
在线安全	98
安全实践和认知	98
安全实践和认知(续)	99
恶意软件和病毒	99
网络钓鱼攻击	99
勒索软件	99
网站篡改	99

附录 2: 事件列表 101

图片清单

图 1. FBI 仇恨犯罪数据: 宗教偏见事件和针对 How 的事件	13
图 2. FBI 仇恨犯罪数据: 因宗教信仰而被杀害的人员	14
图 3. 袭击类型	17
图 4. 按州统计的袭击	18
图 5. 事件时间线	18
图 6. 持枪乱射事件时间线	20
图 7. 袭击前的计划行为	21
图 8. 已知犯罪者的可疑动机	22
图 9. 已知犯罪者报道出的犯罪史	22
图 10. 教派	23
图 11. 与设施的关联	23
图 12. 宗教场所社区	49
图 13. If You See Something, Say Something® 的“5Ws”	51

安全实践

应急行动计划	28
风险、威胁薄弱环节和后果	32
CISA Protective Security Advisors	40
暴力之路	50
练习问候的力量	52
跑开、躲藏、反击	53
减轻暴力强度	54
专业联络伙伴关系	60
拨款资助	64
用设计求安全	64
建立网络攻击应对准备文化	82
CISA Cybersecurity Advisors	83
选择可靠的密码	84
识别网络钓鱼攻击	87

热情的环境并不等于毫无防范。



Assistant Director 来信

宗教自由是美国宪法第一修正案明确规定的自由之一。然而，最近出现了数起对各类教众的袭击，使得全国的宗教场所都面临独特的安全挑战。虽然新冠肺炎疫情让我国民众的面对面聚会暂时受到限制，但美国民众很快就能在自己的宗教社区再次安全聚会，在进行这类聚会时不应心怀忐忑。

The Cybersecurity and Infrastructure Security Agency (CISA) 致力于与宗教社区合作，帮助减轻有针对性的暴力威胁，并做好准备应对可能发生的事件。

我们的首要任务是保护宗教场所的安全，同时保障热情好客、开放包容的环境。本指南介绍了对过去十年一系列事件的全新分析，并提供了一组缓解方案，旨在打造稳健可靠、层次分明的安全途径。

作为 CISA 负责基础设施安全的 Acting Assistant Director，我向您保证，我们将继续努力寻找创新手段，并利用这些创新手段共同减轻整个国家面临的风险。感谢您立志保护我们的国家，感谢您继续为保护美国民众出力献策。

此致，

Scott Breor
基础设施安全 Acting Assistant Director



大纲

针对宗教场所的暴力行为在美国是一个真实且可能日益严重的问题,也是 U.S. Department of Homeland Security (DHS) 的首要任务。作为国家的风险顾问, Cybersecurity and Infrastructure Security Agency (CISA) 编制了本指南,以帮助宗教信仰组织 (FBO) 制定一项全面的安全策略,应对全国每个教堂、清真寺、犹太教堂、寺庙和其他宗教活动场所的独特情况。

为了更好地了解问题的性质, CISA 利用开源研究汇编了 2009 年至 2019 年十年期间发生的 37 起有针对性的暴力事件。从这些案件研究中得出的分析直接为本指南提供了依据,并揭示了几个值得注意的趋势。

- CISA 观察到, 2012 年有针对性的暴力事件大幅增加, 2015 年至 2019 年间事件数量明显增加。这 37 起事件导致 64 人丧生, 59 人受伤。
- 袭击中有 54% (n=20) 是某种武装袭击, 包括枪击、利器和车辆袭击。其中五起袭击属于大规模枪击。
- CISA 确定, 67% (n=25) 的袭击是出于对特定种族或宗教身份的仇恨, 22% (n=8) 与家庭纠纷或个人危机有关。剩余的 11% (n=4) 原因不明。
- 在这些事件已知的 36 名肇事者中, 有 58% (n=21) 参与了某种形式的预谋袭击计划活动。

在这一分析中, CISA 还描述了罪犯经常使用的几种战术和方法。本指南中的安全框架可以加强这些战术和方法所针对的特定薄弱环节。它的基本目标是宗教场所采用这一全面、多层次的安全策略后,可以得到最好的自身保护。

为了制定和实施能够适应各个宗教场所需求的安全计划，CISA 建议采取以下重要的安全措施：

- 清晰确定制定和实施安全措施的角色和责任。
- 评估薄弱环节，了解自己宗教场所面临的风险。
- 确保自己的宗教场所认识到潜在威胁，做好应对紧急情况或事件的准备，并与更广泛的社区建立联系，做好社区准备和防范。
- 采取物理安全措施，监控和保护周边的外部、中部和内部，同时尊重宗教场所每个区域的用途。
- 以儿童安全为重点，采取安全措施保护儿童保育和托儿所设施以及学校。
- 实施网络安全最佳实践，以保护重要信息并防止潜在的网络袭击。

这些安全选项不是万能的，但全面的安全方法是保护人员、财产和数据的最佳解决方案。宗教场所应根据其社区的需求定制这些知识，同时保持开放和热情的氛围，使其成为美国社会结构的重要组成部分。

介绍：保护宗教场所

宗教场所在美国社会中的独特角色

宗教是全国各地社区的强大组织力量。根据 Pew Research Center 的宗教形势调研，估计有 36% 的美国人每周都要参加宗教仪式。加上每月或每年参加的人数，这一数字估计会增长到 69%。在婚礼、葬礼和宗教节日等重要场合，这一数字甚至更高。¹

宗教自由是受美国宪法保护的一项权利，被公认为是美国社会的基本组成部分。宗教组织 (FBO) 在提供食物、住所和衣服等社会服务以及培养社区意识方面发挥着突出作用。对许多人来说，信仰提供了力量和希望；舒适和安心；道德指针和精神指导；帮助战胜压力和恐惧。

这种社区感和目标感通常以宗教场所 (HoW) 为中心。教堂、清真寺、犹太教堂、寺庙和其他宗教活动场所都是热情帮助避难的场所，出入几乎没有限制。无论是哪种信仰，宗教场所几乎总是全面开放的，反映出一种信任和接纳的文化。

但热情的环境并不等于说是毫无防范。

宗教场所面临着独特的挑战，即在安全和便利之间取得合适的平衡。本指南为 HoW 提供了背景和指导，使其能够根据自身情况和环境对最合适的安全级别做出明智的决定。

1 “Attendance at religious services,” Pew Research Center, <https://www.pewforum.org/religious-landscape-study/attendance-at-religious-services/>, (accessed July 9, 2020). 另请参见 “Fast Facts about American Religion,” Hartford Institute for Religion Research, http://hartfordinstitute.org/research/fastfacts/fast_facts.html (accessed May 4, 2020)

宗教场所袭击

在过去的几年里，Charleston、Sutherland Springs、Pittsburgh、Poway 和 Monsey 等城市的宗教场所遭到袭击，引发了全国对暴力、社会冲突和心理健康的关注。

Cybersecurity and Infrastructure Security Agency (CISA) 在此给出的分析指出，在 2009 到 2019 这十年期间此类有针对性的暴力事件的数量一直在增加。这些袭击的性质千差万别，受害者的教派和袭击发生的地理区域也各不相同。

CISA 强调，尽管此类袭击数量似乎在上升，但从统计角度来看，数量并不多。每一次都对直接受影响者和整个社会造成深刻创伤。虽然这些袭击造成了可怕的影响，但仍必需维护社会纽带，使宗教场所成为社区独特而不可分割的一部分。宗教场所可以在不损害其特殊性的情况下采取许多安全措施。本指南旨在帮助宗教场所找到最适合其独特需求和环境的平衡。

Department of Homeland Security 的使命是什么？

Department of Homeland Security (DHS) 确定了六项总体任务，这些任务构成了其战略策略。² 其中三项任务是打击恐怖主义和国土安全威胁，保护网络空间和重大基础设施的安全，以及加强准备和防范，这些任务旨在降低暴力风险，直接接触我们国家的信仰组织和宗教场所，防止针对其成员和设施的袭击。

为了应对最近的这些袭击，DHS 正在加大力度，通过提供信息、培训、演习和专业知识，加强 HoW 的防范和准备，增加缓解资源。2020 年 4 月，该部门指定 Office of Partnership and Engagement (OPE) 领导 FBO 的安全协调工作。2020 年 6 月，DHS 还宣布成立一个 Faith-Based Security Advisory Council (FBSAC)，就与宗教场所、信仰组织和国土安全有关的事项向 Secretary of Homeland Security 提供建议。

CISA 正在努力解决这一紧迫的安全问题，本指南就是措施之一。鉴于这些袭击的性质，DHS 制定本指南也是为更好地了解 and 解决有针对性的暴力行为。³ 宗教场所所有针对性的暴力和安全袭击是联邦政府、州、地方、部落和领土政府 (SLTT) 越来

² “Strategic Planning,” U.S. Department of Homeland Security, <https://www.dhs.gov/strategic-planning>

³ U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, 2019 年 9 月, <https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence>

越重视的问题。U.S. Secret Service (USSS) National Threat Assessment Center (NTAC)、DHS Center for Faith and Opportunity Initiatives 和 U.S. Department of Justice (DOJ) Community Relations Service 为此报告提供了重要的素材。

与恐怖主义行为一样,规划和目标选择是有针对性暴力的标志,为预防、干预和缓解风险提供了重要机会。在本指南中,CISA 考虑了如何将之前关于有针对性暴力(如学校暴力)的一些研究结果应用于宗教场所的安全规划。

CISA 的工作是什么?

CISA 是根据 2018 年网络安全和基础设施安全局法案设立的,负责领导联邦网络安全和关键基础设施安全计划、运营和政策。⁴ 作为国家的风险顾问,CISA 还负责公共集会,这些集会通常很容易进入,安全或保护措施有限。

保护公众集会安全是 CISA 最重要的一项任务,也是行动重点之一。⁵ CISA 与私营实体合作,确定、制定和实施创新灵活的措施来降低包括宗教场所在内的人群聚集场所的风险,从而给予领导和支持。

指南概述

本指南提供了新的分析、建议和资源。最重要的是,本指南还提供了一个概念框架,用于思考 HoW 的安全和制定最适合每个社区独特情况的安全计划。



第 1 章对美国十年来发生的针对宗教场所的暴力行为进行了分析,包括对罪犯最常用战术和方法的概述。此分析的结果为后续章节中所给出的指导提供了直接依据。



第 2 章列出的流程供各个 HoW 用于考虑各自的安全需求,制定稳健可靠、层次分明的安全策略,同时确保宗教场所保留自身特色,仍是当地社区的重要组成部分。

⁴ Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law 115-278, U.S. Statutes at Large 132 (2018): 4168-4186, <https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf>.

⁵ Cybersecurity and Infrastructure Security Agency, Strategic Intent, August 2019, <https://www.cisa.gov/publication/strategic-intent>. 另请参见“Securing Soft Targets and Crowded Places”, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/securing-soft-targets-and-crowded-places>.



第 3 章具体指导如果进行全面的薄弱环节评估,帮助 HoW 评估它们当前的安全态势和具体需求。



第 4-7 章更详细地讨论了安全规划和各个组件的不同方面,它们是 HoW 建立分层安全策略所必需的。



最后是**附录 1**,其中有**资源指南**,完整列出了宗教场所可用于提高其整体安全水平的产品。本章按主题组织资源,以使用户能够浏览对其需求最有利的大量选项和决策点。

读者还可以在**整个指南**中查找精心编排的参考资料和资源。这些资源大部分是由 DHS 和其他安全和执法专业人员提供的,感兴趣的 HoW 可以利用它们进行后续深入研究,继续其战略安全规划。



1

了解问题

介绍

宗教场所 (HoW) 的大小、教派和地理位置各不相同, 每个都有自身独特的安全需求。本指南在一定程度上是直接针对近年来一系列备受瞩目的袭击事件出台的, 这些事件引起了全国的关注, 让各种宗教信仰社区陷入困境。本指南还反映了保护人群的一般最佳实践, 并考虑了 HoW 带来的特殊考虑事项。

为了更好地了解近年来针对宗教活动场所的暴力问题是如何演变的, 并解决全国各地存在的多种安全需求, Cybersecurity and Infrastructure Security Agency (CISA) 彻底查询了有关该主题的文献和学术材料, 以及来自开源研究、媒体报道以及国家数据库的信息, 编制了 2009 年至 2019 年 37 起案件研究事件的清单。结合现有文献, 这些案件研究揭示了可以采取哪些步骤使宗教场所更加安全的高水平趋势和重要教训。

这些教训是本指南所列出的安全选项的直接依据。总之, 这项研究清楚地表明, HoW 面临着各种安全挑战, 需要一种全面、多层次的安全方法。

查询文献和全国的趋势

学者们估计,美国大约有 35 万至 40 万个人会众。¹ 每一个都代表着当地社区的重要组成部分,所有信仰的宗教场所传统上都被视为重视开放和包容的圣地。与此同时,这种开放性、社会声望和象征意义也带来了独特的安全挑战。

CISA 为本指南查询了来自多个领域和学科的文獻,包括:开源媒体报告;同行评审期刊中的学者文摘;政府报告、文件和数据库;以及执法、威胁评估和其他安全专业人员发表的文章。

宗教场所的大小、教派和地理位置各不相同...

总的来说, HoW 安全领域相对较小,关于针对性暴力具体问题的现成文献更少。近年来,安全专业人员越来越关注教堂、犹太教堂、清真寺、寺庙和其他宗教场所的需求,但界内的大多数文献本质上都是预防性的(而不是分析性的)。² 与此同时,学者们刚开始系统地研究针对 HoW 的暴力活动。³ 正如研究人员无法

确切说出美国境内个人会众的精确数量一样,也无法准确计量故意针对宗教场所的暴力行为的数量。

建立稳健的标准化跟踪系统就是一个难题。现有的研究和分析通常来自媒体报道或不相关的数据库,例如, Hamline University 的 *The Violence Project*,⁴ 或 Federal Bureau of Investigation (FBI) 的 Uniform Crime Reporting (UCR) Program, 该方案汇集了地方司法机构报告的仇恨犯罪。⁵ 大多数研究人员认为,这些数据库虽然有用,但由于报告不完整或不一致而受到限制,并假设其中记录的事件可能是不完全统计。⁶

1 C. Kirk Hadaway 和 Penny Long Marler 所著的 “How Many Americans Attend Worship Each Week? An Alternative Approach to Measurement,” *Journal for the Scientific Study of Religion* (2005), 44 (3): 307-322; Simon Brauer 所著的 “How Many Congregations Are There? Updating a Survey-Based Estimate,” *Journal for the Scientific Study of Religion* (2017) 56 (2): 438-448

2 Jim McGuffey、Paula L. Ratliff、Doug Meacham、Phil Purpura、Dick Raisler、Carl Chinn 和 Alistair Calton 所著的 *Securing HoWs Around the World* (ASIS International, 2017), <https://www.asisonline.org/globalassets/get-involved/councils/documents/best-practices-securing-houses-of-worship.pdf>

3 要查看现有学术文献的简要描述,请参见 Christopher P. Scheitle 所著的 “Crimes occurring at places of worship: An analysis of 2012 newspaper reports,” *International Review of Victimology* 22 (1), 2016 年 1 月: 65-74 和 Christopher P. Scheitle 与 Caitlin Halligan 所著的 “Explaining the adoption of security measures by places of worship: perceived risk of victimization and organizational structure,” *Security Journal* 2018 年 7 月 31 日: 685-707。

4 “The Mass Shooter Database,” *The Violence Project*, <https://www.theviolenceproject.org/>

5 “Uniform Crime Reporting Program,” Federal Bureau of Investigation, <https://www.fbi.gov/services/cjis/ucr/>

6 Scheitle 所著的 “Crimes occurring at places of worship: An analysis of 2012 newspaper reports”。

即便如此,数据还表明了两个明显的趋势: HoW 面临的持续有针对性犯罪活动处于起步阶段,有针对性暴力的具体威胁可能会增加。

另一个特点是事件类型,从统计角度看类型是常见的,但不一定威胁生命。例如,可能全国各地的 HoW 都遇到过破坏行为。⁷ 然而, HoW 似乎还面临着一定程度持续威胁生命的暴力,但它们可能未达到本指南中使用的针对性暴力的标准。根据 FBI 的数据估计,2000 年至 2016 年间,每年约有 480 起暴力事件,包括武装抢劫、袭击和爆炸,每年造成 46 人死亡,218 人重伤。⁸

...每个都有自身独特的安全需求。

另一方面,大规模枪击事件的数量在增长,它造成的伤害和死亡是最严重的。在过去五年中,全国大规模枪击事件普遍呈上升趋势,此类袭击事件也随之增加,通常符合对针对性暴力的定义(概述如下)。例如,根据 *Violence Project* 的追踪, Sutherland Springs 的 Baptist 教堂发生的袭击是美国死亡率排第五的大规模枪击事件。⁹

从定性角度讲,社会氛围和对 HoW 的威胁之间似乎存在着紧密的联系。历史分析表明,对不同种族和宗教团体以及个别宗教场所的袭击往往伴随着激烈的种族和宗教冲突。一些众所周知的案例包括爆发反犹太主义和反穆斯林期间焚烧和向黑人教堂扔炸蛋,或损毁和破坏犹太教堂和清真寺。¹⁰

7 Christopher P Scheitle 所著的“Crimes occurring at places of worship: An analysis of 2012 newspaper reports,” *International Review of Victimology* 22 (1), 2016 年 1 月: 65-74; William Bourns 和 Wesley D. Wright 著。“A Study of Church Vulnerability to Violence: Implications for Law Enforcement”, *Journal of Criminal Justice* 32 (2), 2004 年 3 月: 151-157

8 “Serious violence at places of worship in the U.S.—Looking at the numbers”, Dolan Consulting Group, 2019 年 9 月 9 日, <https://www.dolanconsultinggroup.com/news/serious-violence-at-places-of-worship-in-the-u-s-looking-at-the-numbers/>.

9 Jillian Peterson 和 James Densely 所著的“Opinion: Why do people attacks places of worship? Here’s what we know from our mass shootings database”, *Los Angeles Times*, 2019 年 12 月 30 日; Jillian K. Peterson 和 James A. Densely 所著的“The Violence Project: Database of Mass Shootings in the United States, 1966-2019”, 2019 年 11 月,第 16 页, <https://www.theviolenceproject.org/>.

10 要查看选出的更多近期示例,请参见: John P Bartkowski、Frank M Howell 和 Lai Shu-Chuan 所著的“Spatial variations in church burnings: The social ecology of victimized communities in the South”, *Rural Sociology* 67 (4), 2002 年 12 月: 578-602; Yehudit Barsky 所著的“Terrorist Incidents and Attacks Against Jews and Israelis in the United States”, Community Security Service, 2016, <https://jewishspg.org/app/uploads/2018/09/Terrorist-Attacks-Against-Jews-in-US-1969-2016.pdf>; American Civil Liberties Union, “Nationwide Anti-Mosque Activity”, 2019 年 12 月, <https://www.aclu.org/issues/national-security/discriminatory-profiling/nationwide-anti-mosque-activity>.

动荡的迹象指示国家再次进入社会动荡时期,与此同时,出于偏见的袭击和仇恨犯罪也在上升。*Associated Press* 指出,自 2015 年以来,发生了三起针对 HoW 的最致命袭击事件。与此同时,社交媒体的兴起为仇恨言论和仇恨意识形态在互联网的某些角落蓬勃发展创造了肥沃的土壤。¹¹

为了应对这些挑战,Department of Homeland Security (DHS) 投入了越来越多的资源来解决针对性暴力的具体问题,并于 2019 年 9 月发布了打击恐怖主义和针对性暴力战略框架,以更好地协调政府行动。值得注意的是,该报告呼吁人们重新关注源自美国境内的安全威胁。DHS 确定了两大类特别关注事项:(1) 受外国恐怖组织信息和意识形态驱使的本土暴力极端分子(HVE)和(2) 国内恐怖分子,特别是与白人至上主义暴力极端主义有关的恐怖分子。¹² 这两个类别都有可能对 HoW 造成威胁。

此外,新冠肺炎疫情可能会增加仇恨犯罪和种族偏见在西方世界的蔓延,进一步加剧对 HoW 的威胁,并促使 CISA 向宗教组织发出咨询,警告说“疫情造成的压力可能会刺激个人决定发动袭击或影响其选择的目标。”¹³

除了由个人和国内危机引发的更为随机和不可预测的袭击外,图 1 (第 13 页)和图 2 (第 14 页)所示的出于仇恨的袭击日益普遍,这对美国境内的 HoW 来说是一个严重的风险。

11 Adeel Hassan 所著的“Hate-Crime Violence Hits 16-Year High, FBI Reports,” *New York Times*, 2019 年 11 月 12 日; Federal Bureau of Investigation, “2018 Hate Crime Statistics,” <https://ucr.fbi.gov/hate-crime/2018/hate-crime>; Gary Fields 和 David Crary 所著的“Year-end violence highlights danger of worshipping”, *Associated Press*, 2020 年 1 月 1 日; Marc Fisher、Roxana Popescu 和 Kayla Epstein 所著的“Ancient hatreds, modern methods: How social media and political division feed attacks on sacred spaces”, *Washington Post*, 2019 年 4 月 28 日。

12 U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, 2019 年 9 月, <https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence>。

13 Anna Russel 所著的“The rise of coronavirus hate crimes”, *New Yorker*, 2020 年 3 月 17 日; Natasha Bertrand 所著的“DHS warns pandemic ‘stressors’ could trigger attacks on HoWs”, *Politico*, 2020 年 4 月 8 日。

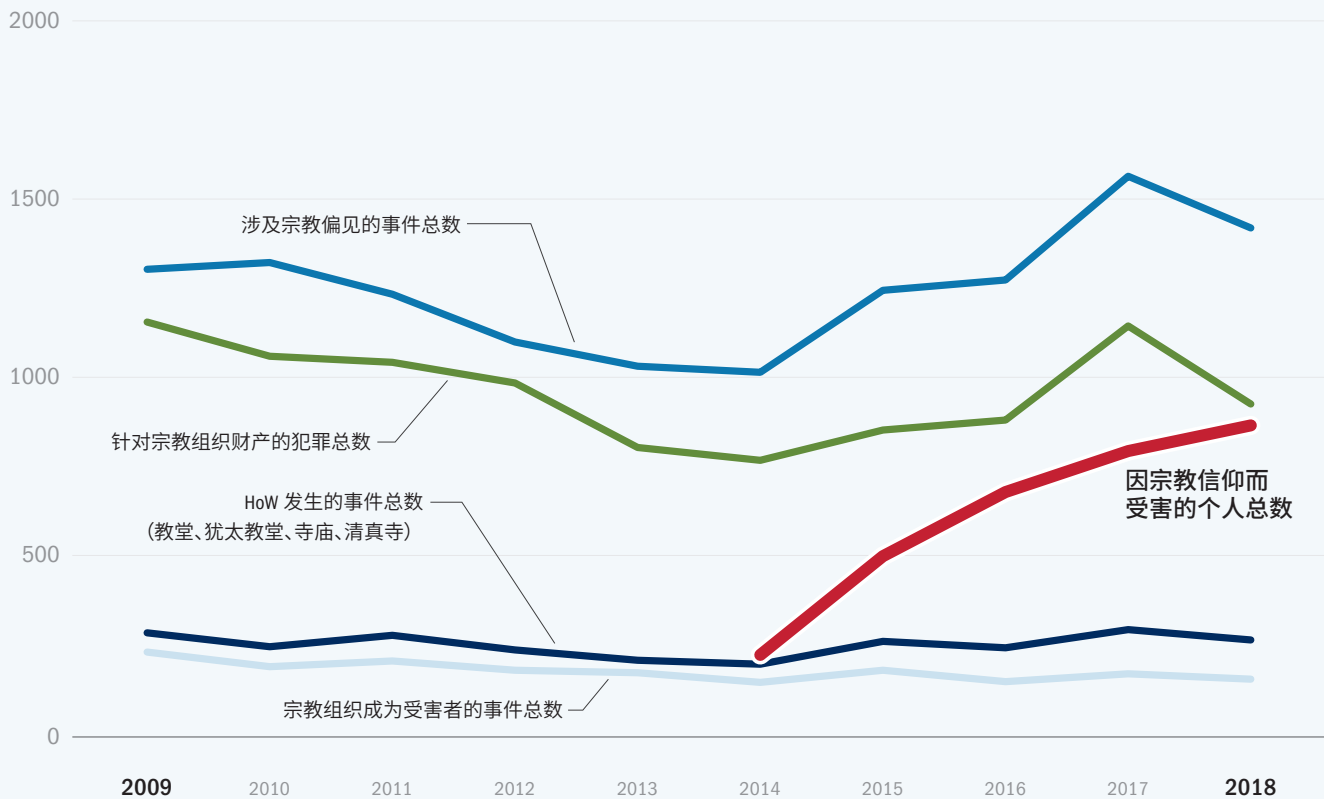


图 1. FBI 仇恨犯罪数据: 宗教偏见事件和针对 HoW 的事件

图 1 显示了 FBI 仇恨犯罪数据中汇编的一系列与宗教偏见有关的类别。中蓝线 (顶部) 追踪了涉及宗教偏见的仇恨犯罪事件的总数。绿线追踪针对宗教组织的财产犯罪数量。红线追踪了因宗教信仰而受害的人数 (包括谋杀/误杀、强奸、严重袭击、简单袭击、恐吓和其他), 这是 FBI 在 2014 年开始设立的一个独特类别。浅蓝色线 (底部) 追踪了宗教组织被记录为受害方的事件数量。深蓝色线 (从下起第二条) 追踪了在 HoW 发生的仇恨犯罪事件的总数。在发布时尚无 2019 年的数据。

这些数据趋势深刻揭示了美国公民生活的总体基调和涉及宗教的仇恨犯罪的普遍性。

来源: FBI UCR 仇恨犯罪统计, 表 1、7、8 和 10 <https://www.fbi.gov/services/cjis/ucr/hate-crime>

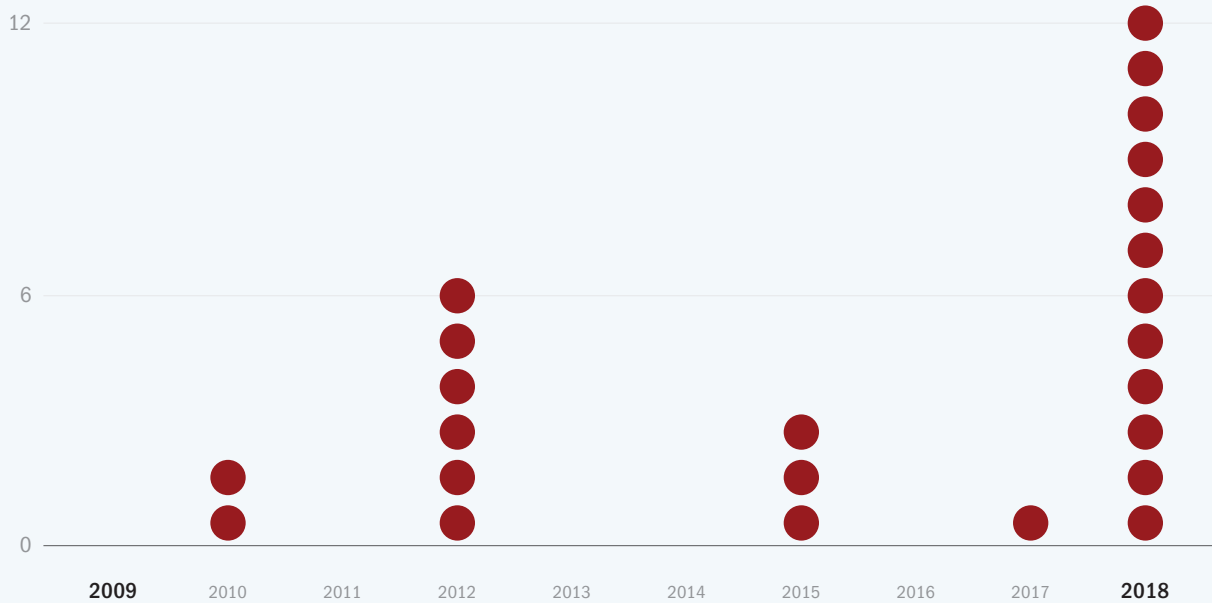


图 2. FBI 仇恨犯罪数据:因宗教信仰而被杀害的人员

图 2 显示了 FBI 仇恨犯罪统计数据追踪的因宗教信仰和偏见而被杀害的人数。这一数字包含在图 1 中宗教信仰受害者总数之内。

来源: FBI UCR 仇恨犯罪统计, 表 7, <https://www.fbi.gov/services/cjis/ucr/hate-crime>

制定案件研究的方法

为了补充现有研究并为本指南中包含的安全注意事项提供背景, CISA 制定了一系列案件研究, 以跟踪 2009 年至 2019 年十年期间针对 How 的暴力行为。CISA 通过搜索多种来源收集了这些事件, 其中包括: FBI 仇恨犯罪统计 (UCR Program 的一部分)、Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Bomb Arson Tracking System (BATS); DHS 的 Technical Resource for Incident Prevention (TRIPwire); the University of Maryland 的全球恐怖主义数据库; 和 Hamline University 的 *The Violence Project*。不过, CISA 的大多数案件研究都来自开源媒体报道, 这些报道提供了最具实质性的公开信息。尽管一些细节有限或不完整, 但 CISA 尽可能通过多个来源证实了基本事实。

为了将蓄意暴力行为与随机犯罪行为区分开来，CISA 使用以下定义作为纳入这些案件研究的标准：**刻意针对美国境内宗教场所或附属财产的暴力行为，导致重大损失、伤害或死亡。**

例如，与 FBI 仇恨犯罪统计数据相比，符合纳入标准的案件数量相对较少，CISA 预计还有其他事件未纳入本指南或未经评估。

针对性暴力

针对性暴力是指目标明确，针对特定个人、群体或地点的暴力。犯罪者选择他们的目标是为了达到特定的动机，例如发泄抱怨或发表政治或意识形态声明。与冲动、随机或自发暴力相比，针对性暴力通常有清晰的迹象或袭击前计划。如果检测到这些行为，则可能有助于阻止或缓解事件。

2019 DHS 战略框架将针对性暴力定义为：

... 涉及国土安全和/或 DHS 活动的任何暴力事件，并且已知或可知的袭击者在暴力袭击之前选择了特定目标。与恐怖主义不同，针对性暴力包括在其他方面缺乏明显的政治、意识形态或宗教动机的袭击，但其严重性和规模足以表明其意图造成与已知恐怖战术相称的大规模伤害、破坏或死亡。¹⁴

案件中纳入的操作定义

为了做此分析，CISA 重点关注了 2009 年至 2019 年期间美国境内发生的事件，并将“针对 HoW 的暴力行为”定义为犯罪者刻意将 HoW 作为目标以期达到以下目的的任何事件：

1. 杀害或伤害一名或多名隶属于 HoW 的人员，包括神职人员、工作人员和会众；
2. 对 HoW 的财产造成重大损坏；和/或
3. 参与针对 HoW 的网络犯罪，包括网络入侵、软件盗版、身份盗窃、金融欺诈和网络钓鱼等行为。

14 U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, 2019 年 9 月，第 4 页。另请参见 Robert A. Fein、Bryan Vossekuil 和 Gwen A. Holden 所著的“Threat Assessment: An Approach to Prevent Targeted Violence,” *Research in Action* (National Institute of Justice, U.S. Department of Justice), 1995 年 7 月。

此分析仅限针对性暴力事件，**不包括**：

- 无法确定犯罪者或无法确定是否专门针对 HoW 的事件；
- 对财产造成轻微损坏的事件；
- 轻微袭击、入室盗窃、涂鸦、盗窃等事件；
- 与帮派暴力或毒品暴力有关的事件，或其他有单独犯罪关系的事件；
- 来自周围社区的暴力行为，偶然侵犯了 HoW 的财产；
- 自发的、冲动的行为，这些行为不是有计划的，也不是专门针对 HoW 的。

事件案件研究

经过详细搜索，共收集了 37 起符合操作定义单独事件。尽管真正全面了解国家趋势需要更多的数据，但这些案件研究展示了过去十年针对 HoW 的暴力行为的大致演变情况。更重要的是，对这些案件研究的深入研究能够深挖攻击者使用的战术和方法。如果运用得当，这些见解可以帮助预测薄弱环节和减轻威胁。

要查看完整的事件清单，参见附录 2。

事件概述

总的来说，CISA 发现针对宗教场所的暴力行为具有宗教、种族和个人意识形态动机，并影响到各种规模和教派的 HoW。如图 4（第 18–19 页）所示，这里展示的事件发生在全国 20 个州，城市和乡村都有。

但案件研究的时间线（图 5，第 18 页）证实了媒体报道的 2009 年至 2019 年 10 年间针对 HoW 的暴力事件有所增加，尽管这一结论并非决定性的。这一时间线表明，尽管这种规模的事件数量不是每年都增加，但在 2015 年至 2019 年间，袭击事件的数量显著增加，这表明针对宗教场所的暴力行为仍然是对美国人民的真正威胁。

袭击类型

CISA 调查了一系列事件,包括实际发生的枪击、刺伤、网络攻击、纵火、爆炸和车辆撞击,如图 3 所示。超过半数(54%, n=20)的案件是某种武装袭击,包括枪击、利器 and 车辆袭击。本研究中包含了一个被挫败的持枪乱射事件,所有 HoW 均可以将它当成降级策略的重要培训工具。

袭击者依靠枪支、刀具、爆炸物或燃烧装置以及网络开发工具等一系列武器进行袭击。枪支是最常用的武器(n=16),随后是燃烧装置(n=6)和网络攻击(n=4)。

图 4 和 5 (第 18-19 页)按每次事件发生的位置和年份描述了袭击。

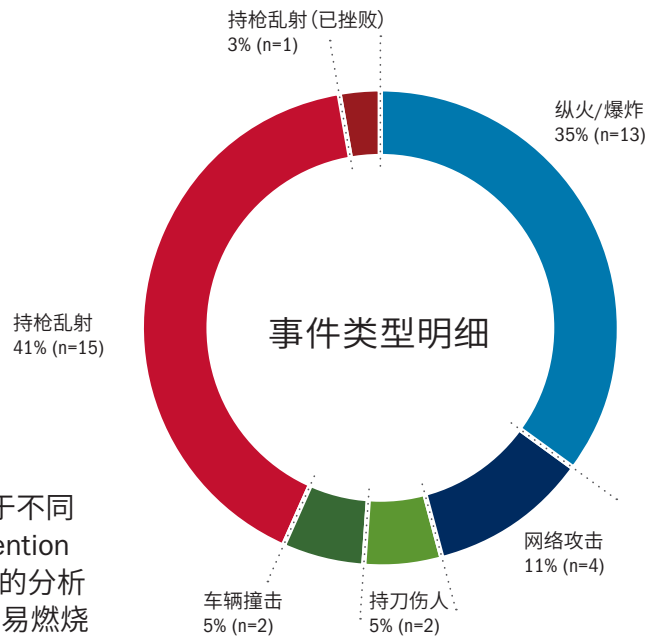
纵火和爆炸

CISA 确定了 13 起纵火或爆炸事件。尽管纵火和爆炸属于不同类型的袭击,但 ATF 和 CISA 的 Office for Bombing Prevention (OBP) 等联邦机构通常对它们一起追踪。对这 13 起事件的分析显示,袭击者使用的装置多种多样,包括助燃剂(n=4)、简易燃烧装置(IIDs),例如瓶装汽油弹(n=6)和简易爆炸装置(IEDs),例如铁管土炸弹(n=1)。其中有一次袭击既使用了 IID 又使用了 IED。其中有三次纵火袭击未报告使用的助燃剂或可燃材料类型。CISA 发现,在这些袭击中,有 85% (n=11) 的动机是对特殊宗教或种族的仇视。

这 13 起事件指示了一个更大的现象。大多数纵火案的目标是正常营业时间后的建筑物,通常是为了造成财产损失。另一方面,在爆炸案中,犯罪者通常有意伤害聚集在特定地点的个人。从历史上看,纵火和爆炸长期以来一直被用来袭击美国的宗教场所,而炸弹威胁往往是恐吓的工具。CISA 预计,在这十年期间,很可能会有更多针对 HoW 的纵火和爆炸案件,但未包括在本分析中。

图 3. 袭击类型

图 3 显示了符合 CISA 针对宗教场所暴力行为标准的袭击类型明细。



纵火和爆炸类型:

- 3  未报告的助燃剂
- 4  使用汽油助燃剂
- 6  简易燃烧装置
- 1  简易爆炸装置



图 4. 按州统计的袭击

图 4 指出了按州统计的袭击 (n=37)。这里展示的事件发生在全国 20 个州, 城市和乡村都有。

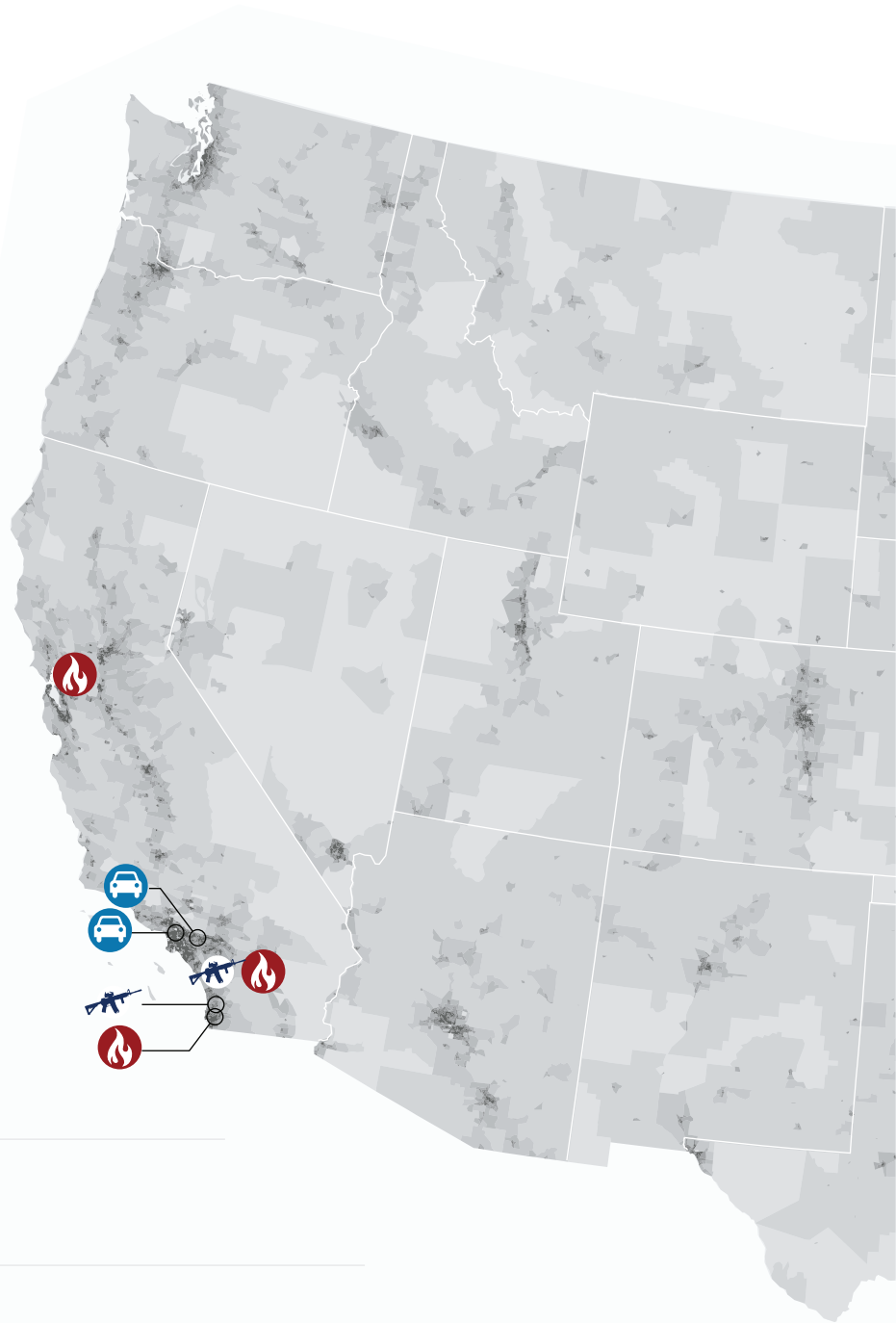
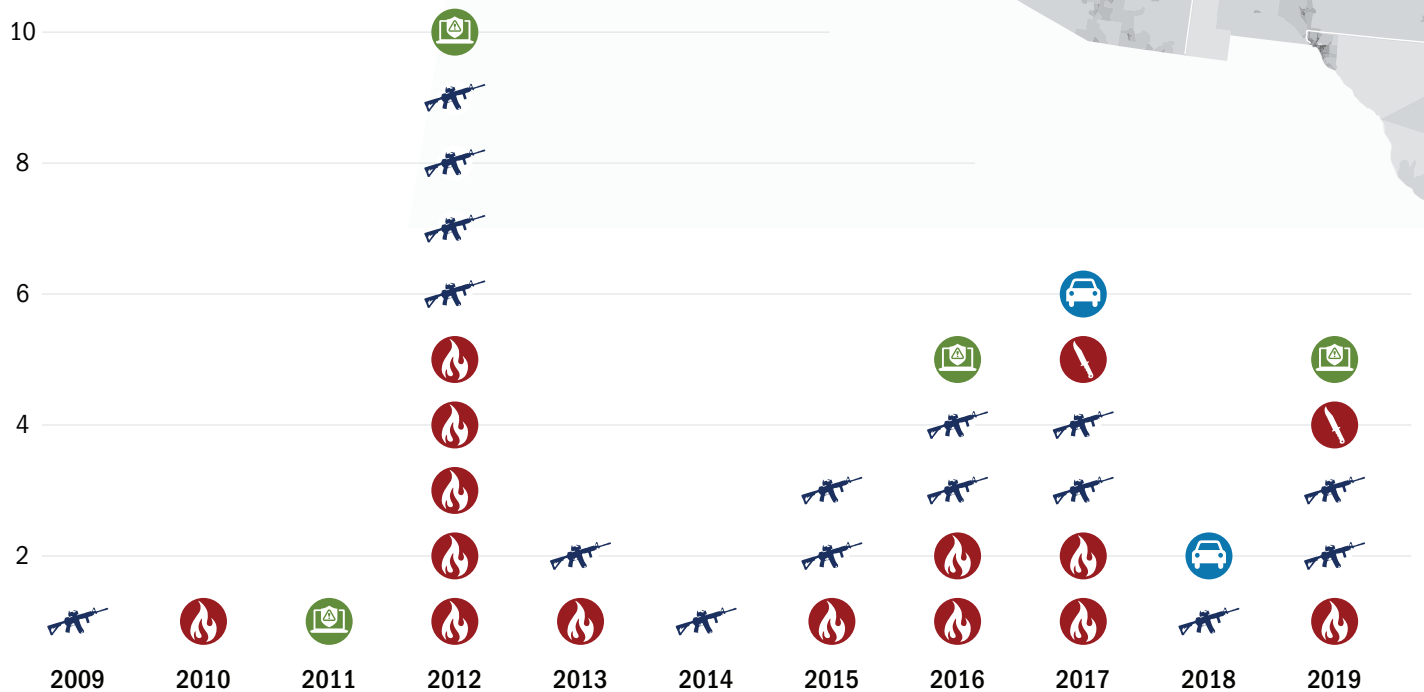
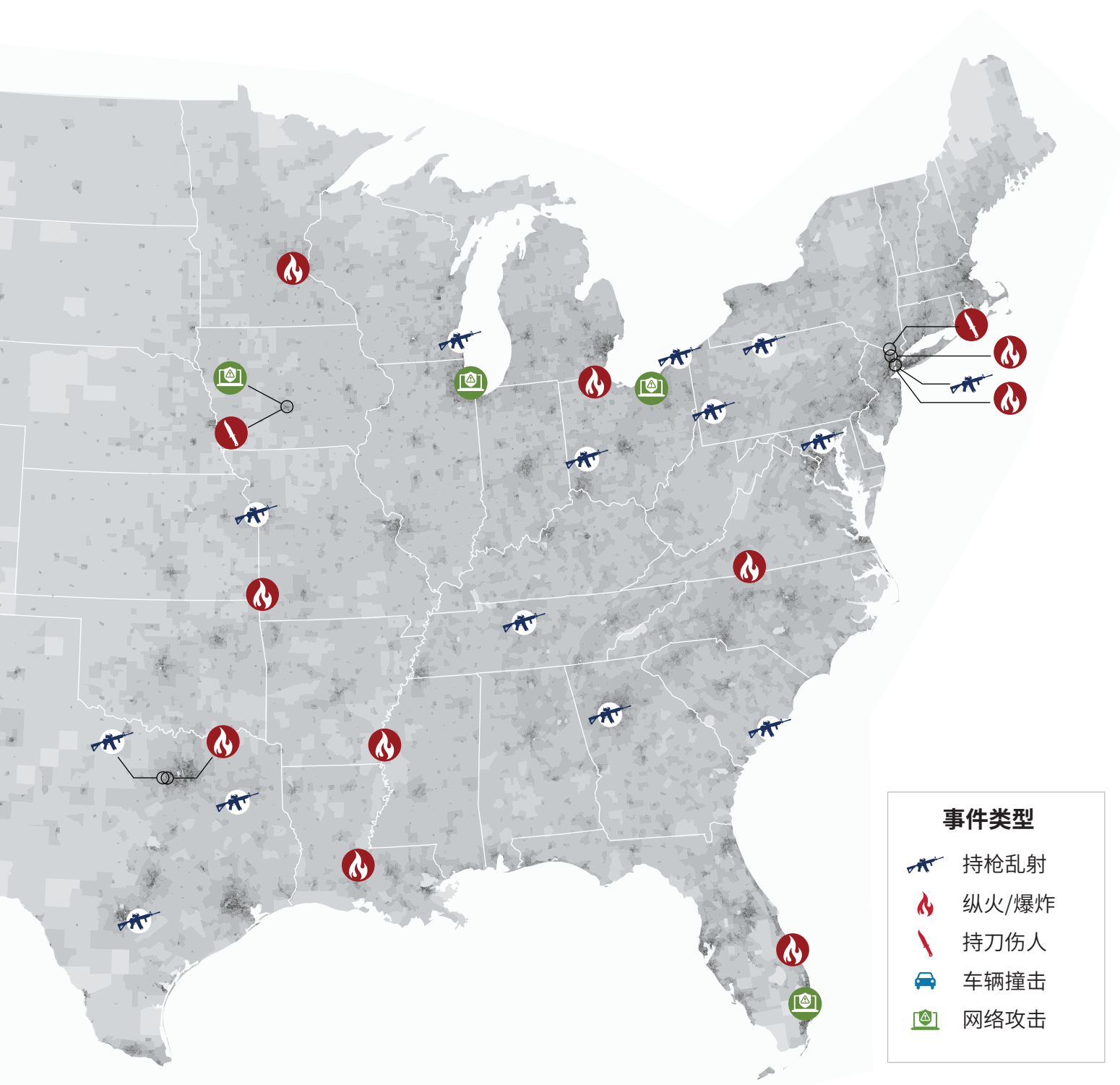


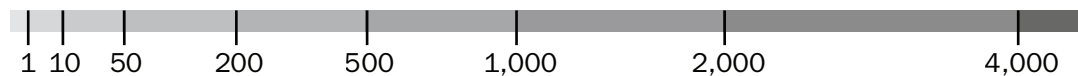
图 5. 事件时间线

图 5 展示了在调研期间事件的时间线 (n=37)。





每平方英里的人口



网络攻击

CISA 审查了四起针对 HoW 的网络攻击,包括两起谋财事件和两起网站篡改事件。HoW 的经济损失分别为 68 万美元和 175 万美元,以及网站篡改造成的担忧和声誉损害。与大多数网络犯罪一样,这些袭击没有已知的犯罪者。网站篡改者和金融黑客是出于意识形态动机还是出于机会犯罪尚不清楚。

武装袭击和大规模枪击

在调查的案件中,有 54% (n=20) 属于某种武装袭击,使用枪支、刀具或车辆故意在 HoW 伤害人员。武装袭击中包括大规模枪击案,它造成的死亡率最高。大规模枪击的定义各不相同,但通常是指使用枪支在同一时间和地点杀死或伤害四个或更多人。本报告包括 15 起持枪乱射事件和 5 起大规模枪击事件。

本报告确定的大规模枪击事件包括几种常见的战术和方法,为我们的许多建议提供了依据。参见图 6 了解这些事件的时间线。

大规模枪击事件:

2012 年 8 月,一名手持手枪的 40 岁男子在 Sikh Temple of Wisconsin (位于 Wisconsin 的 Oak Creek) 开枪射击,随后走进寺庙内继续向会众开枪。警察在枪手离开大楼时与其对峙。枪手共造成六人死亡,包括一名警官在内的四人受伤。枪手在被一名警官射中腹部后自杀。

2014 年 4 月,一名 73 岁的男子手持两把手枪和一支猎枪,在 Kansas 州 Overland 公园的 Greater Kansas City 犹太社区中心停车场开枪,造成两人死亡。随后,他驱车前往附近的 Village Shalom 退休社区,并在停车场开枪,造成一人死亡。没有其他人受伤。警察逮捕了枪手,后来他被判处死刑。

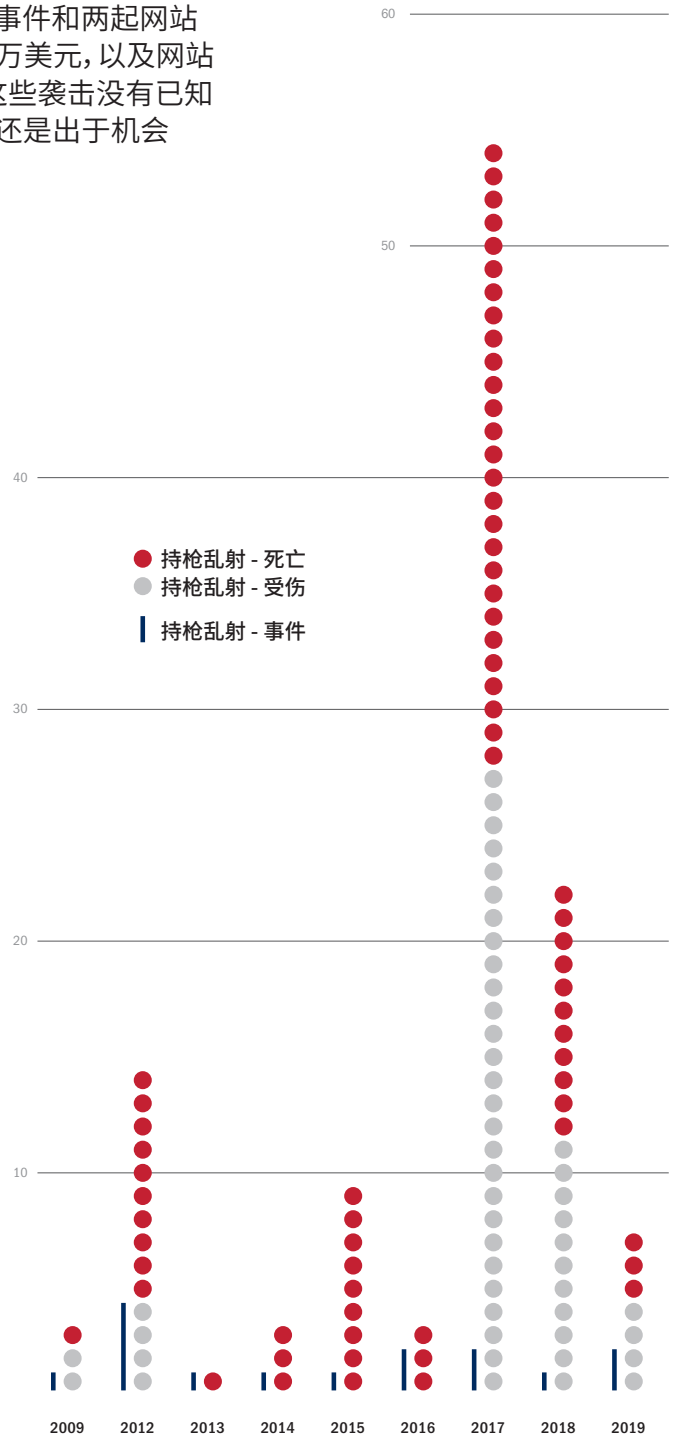


图 6. 持枪乱射事件时间线

图 6 展示了分析中所包含的持枪乱射事件的时间线 (n=15 持枪乱射)。2017 年伤亡人数大幅增加,那是由于 Texas 州的 Sutherland Springs 发生了大规模枪击案,造成 26 人死亡,20 人受伤。

2015年6月,在 South Carolina 州 Charleston 的 Emanuel African Methodist Episcopal Church 教堂举行的祈祷仪式上,一名 21 岁男子手持手枪射击,造成 9 人死亡。枪手逃离了现场,第二天警察将其逮捕。枪手最后被判处死刑。

2017年11月,一名身穿全套战术装备、手持步枪的 26 岁男子下车,在 Texas 州 Sutherland Springs 的 First Baptist Church 教堂外开枪射击。他从侧门进入大楼,继续向聚集在里面的人员开火。在他离开时,一名持枪的邻居与其对峙,引发了一场汽车追逐。这次袭击导致 26 人丧生, 20 人受伤。枪手自杀身亡。这是美国历史上造成宗教场所死亡率最高的袭击。

2018年10月,一名 46 岁的男子手持步枪和三把手枪,在 Pennsylvania 州 Pittsburgh 的 Tree of Life 内开枪射击。共有十一人死亡、六人受伤,包括四名警察。警方在交火后当场逮捕了枪手。检察官指控犯罪者犯有仇恨罪;他正在等待审判。

袭击后果

这 37 起事件造成 64 人丧生, 59 人受伤, 14 起事件造成重大财产损失。每次事件导致 0 到 27 人死亡, 0 到 20 人受伤。与所有其他类型的袭击相比,持枪乱射事件造成的伤亡人数最多。

犯罪者

CISA 确定 37 起事件中有 36 名犯罪者。其中有 30 次袭击是由单个行为者实施的,三名共谋者实施了一次事件,两名共谋者进行了一次袭击,四次网络攻击没有找出犯罪者。36 名袭击者的年龄从 17 岁到 73 岁不等,平均年龄为 38 岁。一名袭击者为女性,其余 35 人均为男性。在 36 名袭击者中,67% (n=24) 是白人,22% (n=8) 是黑人,5% (n=2) 是亚洲人,5% (n=2) 在事件报道中没有指出种族。CISA 使用 U.S. Census Bureau 标准定义本指南中的种族。

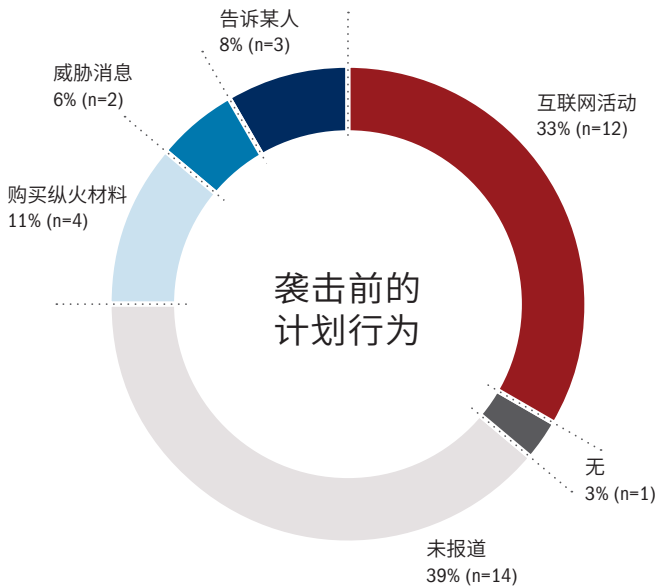


图 7. 袭击前的计划行为

图 7 展示了分析中所含事件的犯罪者的袭击前计划行为。

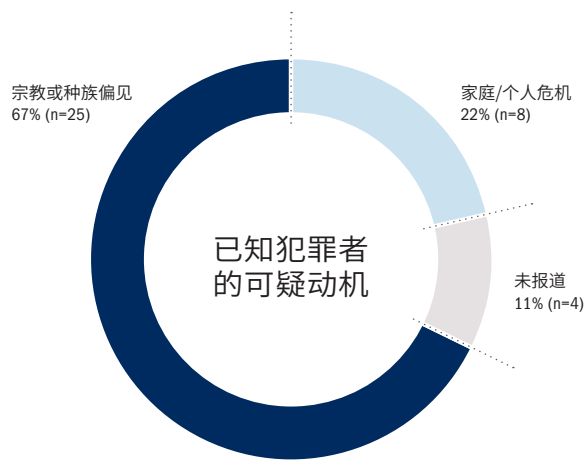


图 8. 已知犯罪者的可疑动机

图 8 展示了 36 个已知犯罪者中每个人的可疑动机明细。

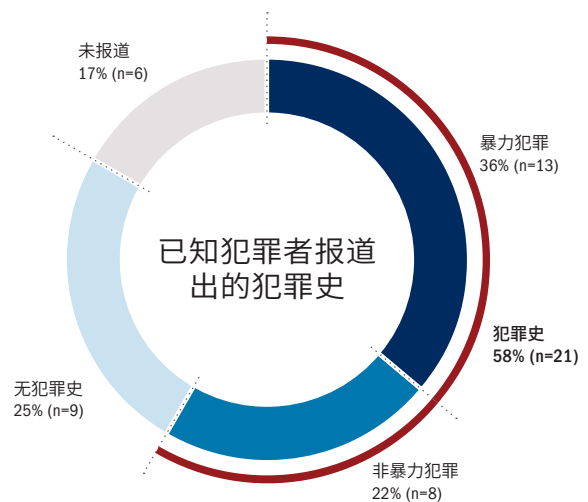


图 9. 已知犯罪者报道出的犯罪史

图 9 显示了媒体报道有犯罪史的已知犯罪者的数量 (总计 58%, n=21), 以及暴力和非暴力犯罪的进一步区别。

媒体报道显示, 58% (n=21) 的犯罪者参与了某种形式的袭击前计划, 表明了他们的袭击意图, 要么直接告诉某人, 要么向 HoW 留下威胁信息, 购买袭击所需的材料 (如燃烧弹), 或者于在线论坛上描述他们的计划。图 7 (21 页) 介绍了这些行为。

CISA 得出的结论是: 69% (n=25) 的犯罪者 (n=36) 的动机是对与目标宗教场所有关的种族或宗教身份的仇恨。袭击者经常在袭击期间或袭击后的评论中透露具体动机, 许多人自称持有仇恨信仰。CISA 确定, 22% (n=8) 的犯罪者的动机是家庭纠纷或个人危机, 包括几起可能的心理健康危机或其他个人压力来源。如图 8 所示, 不同动机往往会产生不同的预先计划行为, 并为早期侦测和干预提供不同的窗口, 如后面章节所述。

犯罪活动史或心理健康斗争史有时可能是未来行为的风向标。在这些案件研究涉及的 36 名犯罪者中, 有 21 人被家庭成员、证人、法院或媒体描述为有某种犯罪史, 根据对事件的报道, 其中 14 人被认为在事件发生前或发生期间经历过心理斗争。参见图 9 了解有犯罪史的犯罪者详细信息。

目标宗教场所

37 起事件的目标分布如下，54% (n=20) 针对基督教机构，24% (n=9) 针对穆斯林机构，19% (n=7) 针对犹太机构，3% (n=1) 针对锡克教机构，如图 10 所示。CISA 的分析发现，65% 的袭击 (n=25) 发生在 HoW 的主楼内；其余事件 (n=12) 发生在相关设施中，如信仰社区中心、住宅、停车场或相关 HoW 计算机系统。

在武装袭击 (n=20) 期间，40% (n=8) 的犯罪者在礼拜期间进入主楼开始袭击。在 45% (n=9) 的武装袭击事件中，目击者或会众试图在警察到来之前与犯罪者周旋。

在所有事件中，有 22% (n=8) 犯罪者之前曾与 HoW 有某种关联，如图 11 所示。在其余的 78% 事件中 (n=29)，之前没有关联，这表明需要如第 4 章所述，制定一个稳健且明确定义的迎接协议。

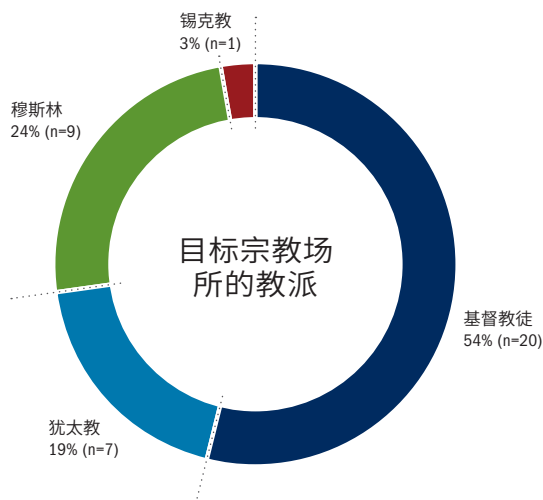


图 10. 教派

图 10 显示了目标宗教场所教派的明细。

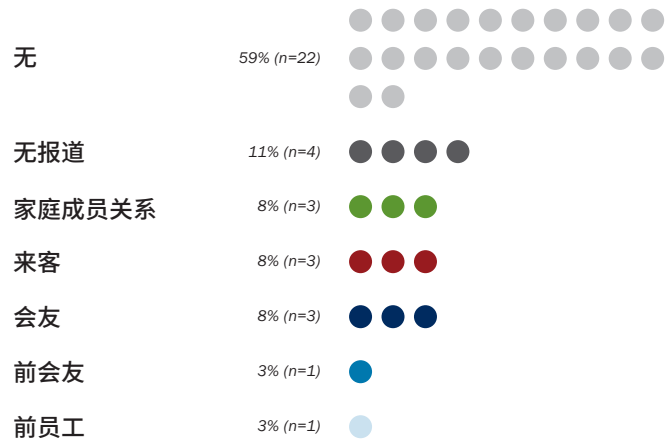


图 11. 与设施的关联

图 11 显示了犯罪者先前与遭受袭击的 HoW 有一定关联的事件数量明细。

犯罪者的战术和方式

在此分析中，CISA 还调查了犯罪者用于实施袭击的战术和方法。HoW 可以借鉴总结出的几项战术和方法来防范或缓解可能的事件。这些包括犯罪者利用的特定薄弱环节，以及 HoW 在促进社区参与时需要考虑的个人行为趋势。

下节简要介绍了几起事件，重点描述了宗教场所在修订其安全程序时可能要考虑的特征。

之前关联

22% 在案件中，有 22% (n=8) 犯罪者之前曾与 HoW 有某种关联。

事件概述

2012 年，一名男子在他们以前的教堂找到了前妻。他在礼拜期间进入大楼，在前妻演奏风琴时开枪打死了她。枪手离开教堂，几分钟后返回，向受害者又开了两枪，随后被目击者制服。

事件概述

2019 年 4 月，有一个人用十个晚上的时间里烧毁了三座历史悠久的黑人浸礼会教堂。这个纵火者在社交媒体上实时发布了犯罪的图片和视频在网上对前两起袭击事件的反应鼓舞下，犯罪者进行了第三次纵火，调查人员将犯罪证据与手机数据以及最近购买的汽油和其他易燃材料联系起来后，将其逮捕。犯罪者对多项仇恨犯罪和纵火指控供认不讳。

行为迹象

57% 在 57% (n=21) 的案件中，犯罪者有过某种形式的规划，揭示出其袭击意图。

19% 在 19% (n=7) 的案件中，犯罪者在与白人至上主义相关的在线论坛上发布了他们的计划。

纵火和爆炸

会众在楼内时发生的爆炸案

8% 在 8% (n=3) 案件中，纵火袭击发生在建筑中有人时。

事件概述

2017 年发生的一起事件中，袭击者打碎了一座清真寺的外窗，并向大楼投掷了一枚铁管土炸弹和一种助燃剂混合物。袭击发生时，拥挤的人在大楼里做晨禱；不过炸弹掷入的办公室空无一人，没有人员伤亡。

宗教场所关门后夜晚发生的纵火

24% 在 24% (n=9) 的案件中, 纵火袭击发生在午夜或非工作时间。

事件概述

2017 年, 一名袭击者在夜间闯入一座教堂, 花了几个小时破坏财产、窗户和家具, 然后在整栋建筑内纵火。警方接到报警有人正在进行入室盗窃, 赶到现场时发现了火情。大火很快被扑灭, 但教堂遭到严重破坏。

事件概述

2014 年的一起事件完全发生在两个不同地点的停车场。袭击者先驱车来到犹太社区中心, 然后在停车场开枪射杀两人。该设施内的工作人员立即启动了封锁程序, 锁住了外门, 并引导游客进入室内。在与一名下班后的安保警察对峙后, 袭击者驱车前往附近的一个退休社区, 在停车场向另一人开枪, 随后被警察逮捕。

武装袭击

袭击在外部发生

11% 在 11% (n=4) 的案件中, 整个袭击事件发生在停车场或建筑的外部。

枪手从外围进入内部圣堂。

8% 在 8% (n=3) 的案件中, 袭击者先是在外围或中围开始袭击, 然后进入宗教场所的内部圣所。

事件概述

在 2017 年发生的这起事件期间, 枪手将车停在教堂外, 等待礼拜结束。袭击者向一名走向自己汽车的妇女开枪, 然后进入宗教场所的正门, 并向圣所内的另外六人开枪。事件发生后, 宗教场所进行了改建, 包括对布局进行调整, 以便会众在礼拜期间可以看到正门。

事件概述

2019 年 12 月, 一大群人聚集在一位纽约拉比的家中庆祝光明节的结束, 当时一名精神失常的男子进入家中, 用砍刀袭击了聚会。会众进行了反击, 在随后的混战中有几人受了重伤; 一名男子后来因伤势过重死亡。袭击者逃离并试图进入隔壁的犹太教堂, 但发现门被听到骚乱的人锁上了。袭击者逃走, 随后被警方逮捕。

袭击不是在正式礼拜时发生

14% 在 14% (n=5) 的案件中, 袭击发生在主要礼拜活动之外。

枪手在礼拜开始后进行袭击

19% 在 19% (n=7) 的案件中, 袭击发生在主要礼拜活动期间。

事件概述

2017 年 9 月, 一名手持两把手枪的男子在礼拜将要结束时走近一座教堂。这名男子蓄意为 2015 年 Charleston 教堂枪击案复仇, 在停车场开枪打死了一名女子然后, 他从后门进入大楼, 开枪打伤了另外六人。一名门卫与枪手对峙, 枪手在搏斗中意外开枪射中自己。门卫制服了受伤的枪手, 直到警察赶到。

事件概述

2019 年, 一名枪手在一个重要的宗教节日进入一个宗教场所, 携带战术装备、一支冲锋枪和至少 50 发弹药。在枪支卡壳前, 袭击者开枪杀死一个, 杀伤三个, 然后逃离现场。

袭击者在 HoW 人员众多时 (例如, 假日礼拜) 发起袭击

22% 在 22% (n=8) 的案件中, 袭击发生在宗教假日或宗教假日前后。

枪手在发起袭击前一直坐等礼拜仪式完成

8% 在 8% (n=3) 的案件中, 袭击发生在犯罪者坐等部分礼拜仪式完成后。

事件概述

在 2019 年的一起事件中, 枪手坐等部分礼拜活动完成, 然后拿着猎枪站起, 将附近的一个人射杀。袭击者着装得很怪异, 他的可疑行为引起了 HoW 志愿者安保团队的注意, 他们立即做出反应并制服了袭击者。

事件概述

在 2012 年的一个宗教节日期间, 一个宗教场所成为网络攻击的受害者, 在这次攻击中, 一名不知名的袭击者破坏了 HoW 的主页, 并将访问者重定向到一个表示支持知名恐怖组织的网站。网站遭到篡改, 其中包括令人不安的图片和来自网络攻击者的吹嘘信息。

网络攻击

网站篡改

5% 在 5% (n=2) 的案件中, 袭击涉及篡改 HoW 网站。

金融欺诈

5% 在 5% (n=2) 的案件中, 袭击涉及金融欺诈。

事件概述

2019 年, 一场网络钓鱼以一个宗教场所为目标, 伪造供应商的电子邮件, 将 HoW 的每月付款重定向到一个欺诈账户。这次袭击造成了巨大的经济损失, 直到真正的公司打电话询问逾期付款的情况时才发现。

战术和方法

战术或方法	事件百分比	建议	事件说明
行为迹象			
犯罪者有指示其袭击意图的规划行为	57% (n=21)	 可疑活动侦测培训 第 4 章	超过半数的犯罪者通过行动或语言揭示出其意图。
之前关联			
他们之前与 HoW 有过一些关联	22% (n=8)	 接待员培训健康计划 第 4 章	很多袭击者 HoW 社区成员都是认识的,但大部分之前没有关联。
武装袭击			
袭击在外部发生	11% (n=4)	 门禁 第 5 章	持枪乱射和车辆袭击完全发生在停车场或 HoW 大楼的外部。
枪手在发起袭击前一直坐在礼拜人群中	8% (n=3)	 接待员培训 第 4 章	在每个案件中,袭击者都是先等礼拜仪式部分完成后开始袭击教众。
枪手从外部进入内部	8% (n=3)	 持枪乱射应对培训和门禁 第 4 章和第 5 章	在每起案件中,袭击者都首先在停车场开枪,然后进入主圣所内部后继续袭击。
在礼拜期间,枪手在主楼内部开始袭击	19% (n=7)	 持枪乱射应对培训 第 4 章	袭击者进入主楼的唯一目的是不分青红皂白地伤害会众,或者因为他们的个人目标就在那里。
袭击者在预计人数比正常时间多时(例如,假日礼拜)进行袭击	22% (n=8)	 在举办繁忙活动期间加强安保 第 4 章	犯罪者计划对密集的会众发动这些袭击。
袭击发生在非礼拜活动期间(例如,伙伴团体、社区剧院)	14% (n=5)	 第 4 章	袭击者选择在小型聚会期间袭击会众。
纵火和爆炸			
会众在楼内时发生爆炸	8% (n=3)	 可疑活动侦测培训 第 4 章	犯罪者意图在礼拜期间实施袭击,从而尽可能多地伤害会众。
宗教场所关门后夜晚发生的纵火	24% (n=9)	 外部照明可视 CCTV 第 5 章	大多数纵火案发生在正常工作时间之后,往往造成严重的财产损失。
网络攻击			
谋财(例如勒索软件、网络钓鱼)	5% (n=2)	 网络适应力 第 7 章	谋财导致近乎 250 万美元的损失。
网站篡改	5% (n=2)	 网络适应力 第 7 章	在两起案例中,犯罪者篡改了网站来显示支持外国恐怖组织。

安全实践

在下面的章节中，CISA 重点介绍了常用最佳实践和案例研究中的例子，在这些示例中，HoW 有现成的工具和步骤，在发生袭击时可以有效应对。一些设施指定了安全主管，并制定了正式的培训方案；另一个组织组建了志愿者安全小组，定期进行应急响应演习，并在事件中保护了其他会众。一些设施在袭击开始后启动了封锁程序。在一些案件中，持枪乱射应对培训起到了挽救生命的作用，因为负责人和会众知道如何应对，以及如何帮助他人逃跑或躲藏。调出“安全实践”来查看得到的经验和最佳实践。

根据确定的战术和方法，CISA 对 HoW 的建议包含了许多具体的指导方针，用于制定分层安全战略、评估薄弱环节、发展组织安全文化、加强人身安全、加强网络安全准备，以及在适用的情况下为托儿所和学校安全制订指南。



总结

这里给出的案例研究简要介绍了在过去十年美国发生的针对 HoW 的暴力事件。尽管从统计角度看数量不多，但每一起案件都对被害人和整个社会造成了深刻伤害。虽然有巨大的痛苦，但我们能从每起案件了解塑造美国社会的力量、袭击者的动机，最重要的是，了解宗教场所可以采取哪些措施来更好地保护生命和财产。

应急行动计划

一次袭击发生后，附属社区中心在数小时内为受害者及其家人提供了关键的援助。社区中心负责人强调，有现成的应急计划对于保护和照顾受害者至关重要。





2

制定整体安全方法

介绍

专家反复强调宗教场所 (HoW) 需要采取分层形式的整体安全方法。¹ 对于缺乏特殊专业知识的社区来说, 这项任务似乎既艰巨, 又会耗资巨大。不过, 如果有合适的参考框架, 制定全面的安全战略会相对简单, Cybersecurity and Infrastructure Agency (CISA) 可以提供帮助。

CISA 在本章提供了一个框架, 用于考量 HoW 的安全和开始未来规划。

安全规划要在成本、文化和需求之间求得复杂的平衡。解决这些相互冲突的需求并做出合理、具有成本效益的决策, 最可靠方法是在深刻理解安全规划基本情况和每个宗教场所面临的独特挑战后, 制订相应的计划。

什么是整体安全方法? 如何实现这一方法?

安全专业人士有时会谈到企业安全的概念, 这是一个在网络领域最常使用的术语。在实践中, 它仅是指采用全面的方法来应对整个企业的安全需求。

这一理念的另一种思考方式是将 HoW 的安全视为一项整体工程, 依赖其各个部分的总和, 并涵盖建筑物、社区和活动的各个方面。您机构的每个方面和每项活动都需要一些保护措施。与此同时, 还必须知晓您 HoW 可能出现的各种威胁、风险和薄弱环节。

**有效的安全
计划从来不是
一维的。**

¹ Hady Mawajdeh 所著的 “Experts Encourage Layered Approach to Church Security Protocols,” *NPR*, 2020 年 1 月 3 日; Scott Stewart 和 Fred Burton 所著的 “Security at Places of Worship: More than a Matter of Faith”, *Stratfor*, 2009 年 6 月 17 日。

在实践中, 寻求解决方案并制定全面的安全策略意味着考虑(或重新审视) 确保宗教场所安全所需的一系列措施, 包括物理安全、网络安全、社区意识、活动规划、事件管理、应急准备、政策制定、培训和人力资源。

本章的其余部分概述了关键概念、注意事项和不同的步骤, 它们将帮助您制定一种稳健、包容和多层次的安全方法。

关键概念、术语和问题

保障会众安全所必需的一系列措施可能让人眼花缭乱。首先提问一组基本问题, 帮助清晰了解您当前的安全状况和任何可能需要的改变:

- 您面临哪些威胁? 有哪些薄弱环节?
- 给定威胁发生的可能性有多大?
- 如果发生这些威胁, 会有何后果?
- 您所在的社区对相关后果的容忍度是多大?
- 您所在的社区对安全实践有何态度?
- 您拥有哪些人力资源来指导、管理和监督安全操作?
- 您有多少预算来支持短期和长期的安全活动?

类似这样的问题会为任何类型的企业安全项目提供依据。由于面临特殊的威胁以及人们普遍倾向于要有开放、和平和热情的气氛, 宗教场所还有其他一些特殊的注意事项。

着手启动这一流程时, 务必考虑以下动态, 为您的总体策略和方法提供依据:

风险、威胁薄弱环节和后果

风险、威胁、薄弱环节和后果都有重要的特点, 在制定安全策略时应牢记这些特点。可以它们之间的关系视为: $风险 = 威胁 \times 薄弱环节 \times 后果$ 。

The Department of Homeland Security (DHS) 专门定义了这些术语, 如下所示:

风险: 有可能因事件、活动或发生事项导致意外结果, 由其可能性和相关后果确定。风险与威胁、薄弱环节和后果密切相关。

威胁: 具有或表明有能力和意图危害生命、信息、操作、环境和/或财产的自然或人为事件、个人、实体或行动。

薄弱环节: 使实体易于被利用或易受给定危险影响的物理特征或操作属性。

后果: 事件、事故或发生情况的影响。

U.S. Department of Homeland Security, *DHS Risk Lexicon*, 2010 版 (2010 年 9 月), <https://www.cisa.gov/dhs-risk-lexicon>

针对 HoW 的暴力行为的特性。 作为宗教活动地, 宗教场所在其社区内具有重要的象征意义, 因此可能成为潜在犯罪者的袭击目标。CISA 的分析明确表明, 大多数针对 HoW 的暴力事件是意识形态或个人危机所致, 其中一些可以在早期发现和制止。

认识威胁。 大多数宗教场所通常都与他们所服务社区的节奏和态度相适应, 是社会结构的重要组成部分。通过提高对可能预示暴力事件的社会紧张局势或个人危机的认识, 承担这一角色可以帮助大大改善安全状况。

制止可疑威胁的能力。 虽然社区参与是提高认识的最佳方式, 但与其他宗教场所 (包括不同信仰的宗教场所)、社区团体、执法部门和社会服务提供方建立正式伙伴关系往往是应对潜在威胁所必需的。在此流程中, 应评估 HoW 所保持的正式伙伴关系类型。

方便、开放和安全之间的平衡。 没有哪个宗教场所愿意变成堡垒。您必须与社区合作, 根据自己的价值观, 自己决定如何在安全的环境和开放的环境之间取得平衡。但选择不是绝对的, 本指南中的框架旨在帮助您找到适合自己宗教场所的平衡。

这些都是复杂的问题, 需要内部审议、哲学讨论、成本效益分析, 并最终在每个宗教场所的关键利益相关方之间建立共识。有效的安全计划绝不会是一维的, 要经过反复的讨论和评估, 这是最基本的要求。

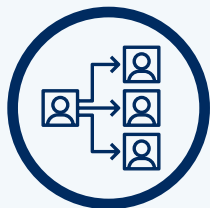
CISA 的 **宗教场所: 家乡安全报告系列** (2017 年 5 月) 专门对宗教社区如何进行联络、计划、培训和报告来改进安全给出了指导, 非常适合用于考虑这些特殊的注意事项。CISA 会继续为信仰组织和 HoW 开发一套安全资源。



在整个报告中查找突出
显示资源的红色箭头
来了解更多信息

宗教场所安全框架

设立岗位和职责



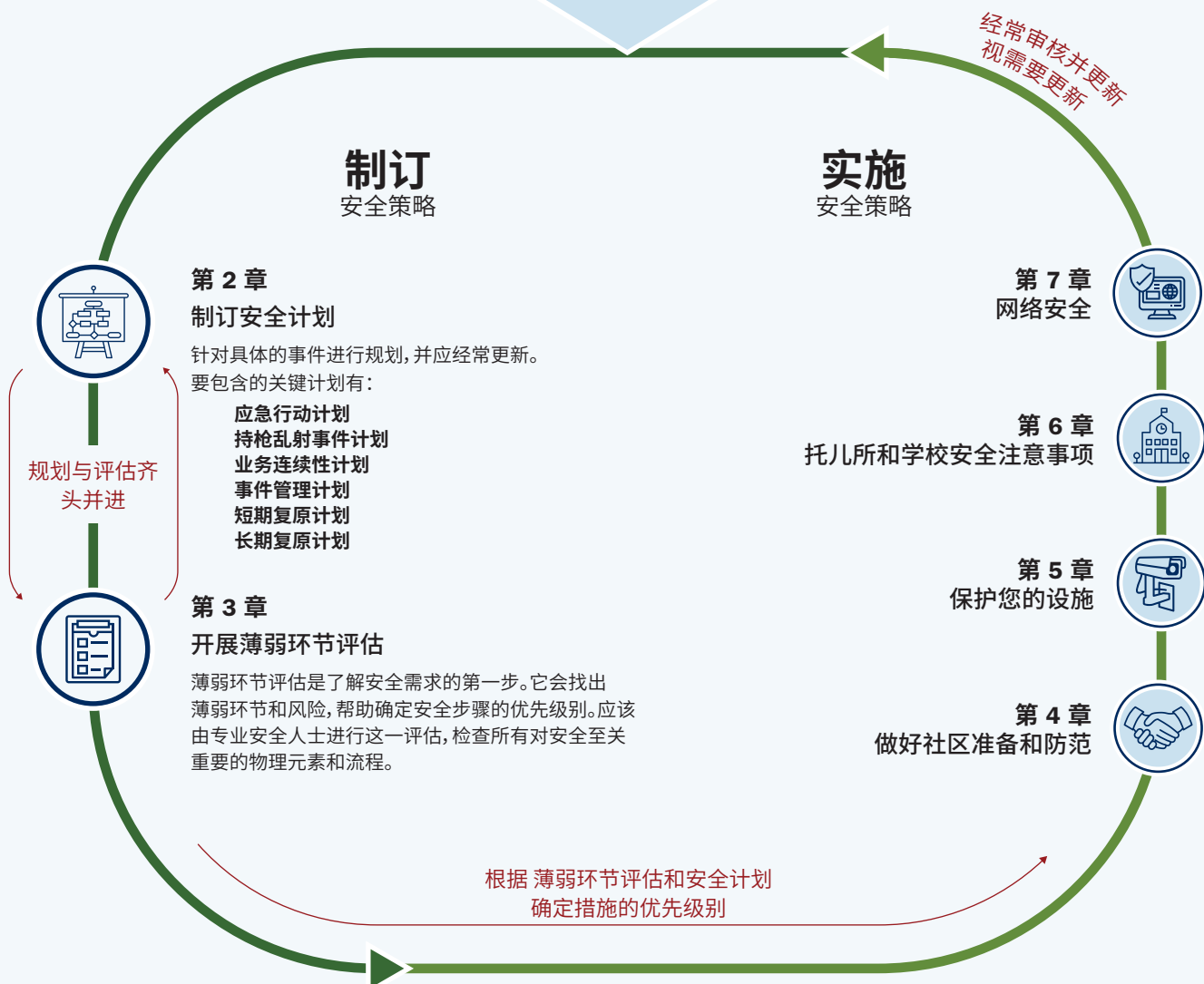
安全协调员
负责实施安全策略。



安全规划团队
通过规划和执行安全策略支持安全协调员。最好有安全经验，但不是必需的条件。



安全团队
包括接待员和志愿者，是找出和报告可疑活动的第一道防线。



制订整体安全策略的框架

CISA 在指南的剩余内容中给出几个重要步骤建议,帮助宗教场所出台整体安全策略。此流程首先为实施安全程度设立清晰的岗位和职责,并要求定期评估。

入门: 设立岗位和职责

设立明确的岗位、职责和预期是取得成功必不可少的条件。制订整体安全策略的第一步是确定由谁监督方案。虽然每个 HoW 的具体职责和头衔可能各不相同,但通过都是由安全协调员主要负责对与安全有关的问题做决策,并负责监督安全方案的日常细节。理想状态是由具备安全经验的全职或兼职工作人员或志愿者担任这一职位。

规划是流程中最重要的一环之一。

CISA 建议成立一个安全规划小组,通过进行研究、评估需求、提供建议和协助制定计划来支持安全协调员。这个团队应该是 HoW 的代表,由神职人员、工作人员和会众组成。安全规划小组可以为多种目的服务,并应帮助承担规划和实施的责任。

在为这些职位确定候选人时,考虑调查您的员工和成员,找出其经验可以为规划过程提供信息的内部专业人员。例如,如果社区有安全、执法、心理健康、应急准备或事件管理专业人员,他们的知识和专业知识可以让您的工作受益,并帮助建立正式的合作伙伴关系。其他宝贵的技能包括政策制定、战略规划、财务和会计以及培训。其中一个挑战是设计一个鼓励批判性思维和创新流程,同时还要下放权力以避免志愿者负担过重。

此外, CISA 鼓励 HoW 考虑与其有关的更多人的安全,例如会众、志愿者、迎宾员、门卫和维护人员等。该小组可以组成更大的安全小组,协助实施安全保障计划。安全协调员和安全规划小组负责大部分决策,安全小组主要负责创建更广泛的安全文化,并确保整个 HoW 社区关注安全话题。话题可以包罗万象,从接待员识别可疑活动,到确定没有活动时由谁来锁门。

规划流程

有效的安全策略需要时间来制订和实施,规划是流程中最重要的一环之一。鉴于目标是制订长期全面策略,所以精心完成每个步骤比抢时间更加重要。

规划阶段有两项齐头并进的主要活动。此流程开始时的主要目标是找出薄弱环节,然后开始制订相应的解决计划。

每个宗教场所的需求都不同。

第 3 章更详细地介绍薄弱环节评估,帮您找出所在社区可能存在的具体威胁及可能面临的特定风险。薄弱环节评估是规划流程的第一步;下一步是开始制定解决这些薄弱环节的计划,并实施动态和多层次的安全策略。

薄弱环节评估和规划是两项不同的任务,但关系密切。两者互通有无,在许多方面,由于响应型安全策略的一个重要特征是经常重新评估需求和调整计划,所以规划流程绝不会终止。

随着您在更大的规划流程中取得进展并开始实施自己的安全策略,您可能还需要考虑针对特定类型的情况和事件制定一些相关计划。要更多了解高级规划,参见第 4 章。

整体安全策略的构件: 如何保障宗教场所的安全

规划流程要经历很长时间,也是长期策略的一部分,薄弱环节评估可能会揭示一系列(可能很多)需求和愿望。有些可以立即解决,有些可能需要更多时间。您的所有计划都需要一定程度的组织和优先级设定。本指南旨在帮您做出这些必要的调整。

本指南的其余每个章节分别讨论整体安全策略的一个关键构件,并尽可能突出联邦资源,所有这些都全面强调制定一种周到、包容和多层次的安全规划方法。



第 3 章更详细地指导如何开展全面薄弱环节分析,它会帮助您了解您的 HoW 可能会如何暴露在风险之下。



第 4 章介绍了做好社区准备和防范如何通过教导社区、建立合作伙伴关系，以及对宗教场所内的惯例和行为做出更改，从而提供保护。



第 5 章提供了保护您的设施使用的框架，并鼓励 HoW 思考如何通过沿房产、地面和建筑物的外部、中间和内部边界进行改造，从而加强物理安全。



第 6 章概述了需要特别关注的托儿所和学校安全注意事项（如适用）。



第 7 章介绍宗教场所网络安全入门知识。这个薄弱环节往往被忽视，但可以通过开发净网文化和应用一些现成的免费资源来解决和缓解。



最后是**附录 1**，其中有资源指南，完整列出了宗教场所可用于提高其整体安全水平的产品。

总结：出台整体安全策略

安全规划是一项复杂的工作，宗教场所的需求各不相同。CISA 不是要提供一份万能指南，而是提供一个综合框架，用于开发可靠的整体安全策略。尽管您的宗教场所遭受袭击的可能性很小，但如果发生事件，这里描述的准备工作的准备工作可以挽救生命，处理紧急情况。



3

开展全面薄弱环节评估

介绍

执行全面薄弱环节评估是制订稳健安全方案的关键步骤，这一流程与调查结果同样重要。此处描述的评估确定现有的安全特征和做法，找出当前的威胁和薄弱环节，并重点指出需要改进的领域。

评估应考虑每个宗教场所 (HoW) 特有的威胁环境，权衡出现持枪乱射、车辆撞击、简易爆炸装置 (IED) 或车载 IED (VBIED)、纵火、利器和网络攻击等情况的可能性。场地中拥有学校或托儿所设施的 HoW 应了解与教育机构相关的独特挑战，参见第 6 章了解这些类型设施的专用防卫指南。

- ▶ 本章提供的薄弱环节评估模型和 Cybersecurity and Infrastructure Security Agency (CISA) 的安全自我评估工具如何支持此流程的系统化方法。各种类型和规模的组织都可以利用这些工具和其他可用的工具和资源来定制评估流程，制定强有力的安全策略，并指导人员和财政资源的分配，以实施该策略。定期审核评估结果有助于应对不断演变的威胁，并确保安全措施能对当前的威胁环境做出反应。

分配岗位和职责

薄弱环节评估的第一步是确定流程的负责人。组织的规模、位置和可用资源都是主要的考虑因素，可以奠定薄弱评估的框架，帮助决定由谁担任这一角色。

理想状态是由安全协调员在安全规划小组的支持下领导这一流程。分担决策责任有助于确保结果得到共识，且因评估产生的任何变动均能得到 HoW 社区的支持。

如果安全挑战看起来相对简单，例如对于小型农村 HoW，则可以在内部进行薄弱环节评估。

CISA PROTECTIVE SECURITY ADVISORS (PSAs)

PSA 是主题专家,在薄弱环节缓解和重大基础设施保护方面受过专门的培训。PSA 与 Department of Homeland Security (DHS) 的其他办事处协调,协助在当地开展 CISA 现场活动。他们还为州、地方和私营部门官员以及重大基础设施所有者和运营商提供建议和协助。PSA 经常为宗教场所和学校评估薄弱环节。

要了解 PSA 的更多细节,请访问 [HTTPS://WWW.CISA.GOV/PROTECTIVE-SECURITY-ADVISORS](https://www.cisa.gov/protective-security-advisors) or contact CENTRAL@CISA.DHS.GOV。

如果评估涉及更复杂的安全环境,如在大教堂、密集的城市地区或特别引人注目的 HoW,可以考虑联系 CISA PSA,帮助设计一个可以由志愿者小组执行的定制流程。

确定薄弱环节评估的范围

根据您的组织特定的兴趣和需求定制薄弱环节评估。要确定评估的范围和复杂程度,考虑提问以下问题:

- 您为什么现在做这项评估?
- 您先前是否做过类似的评估?如果有,您是如何使用评估结果和建议的?
- 您是否已经找出了具体的威胁或薄弱环节?您所在的组织过去是否遇到过暴力威胁或暴力事件?
- 您 HoW 的位置和规模会如何影响您对安全的关注?
- 您所在的当地社区是否面临可能影响您 HoW 社区的安全问题?
- 您是否有安全措施预算?如果没有,将来是否会有为安全计划预算的机会?

这些问题的答案将有助于定义您的评估范围,并制定一个涵盖组织安全态势各个方面的流程。理想情况下,这将产生对优先事项、期望与需求、短期和长期目标、预算考虑和可行性的明确循证决策。在许多情况下,这一流程将产生实施起来相对简单的措施。其他评估结果可能更复杂,需要外部资源的介入,例如 CISA PSA。

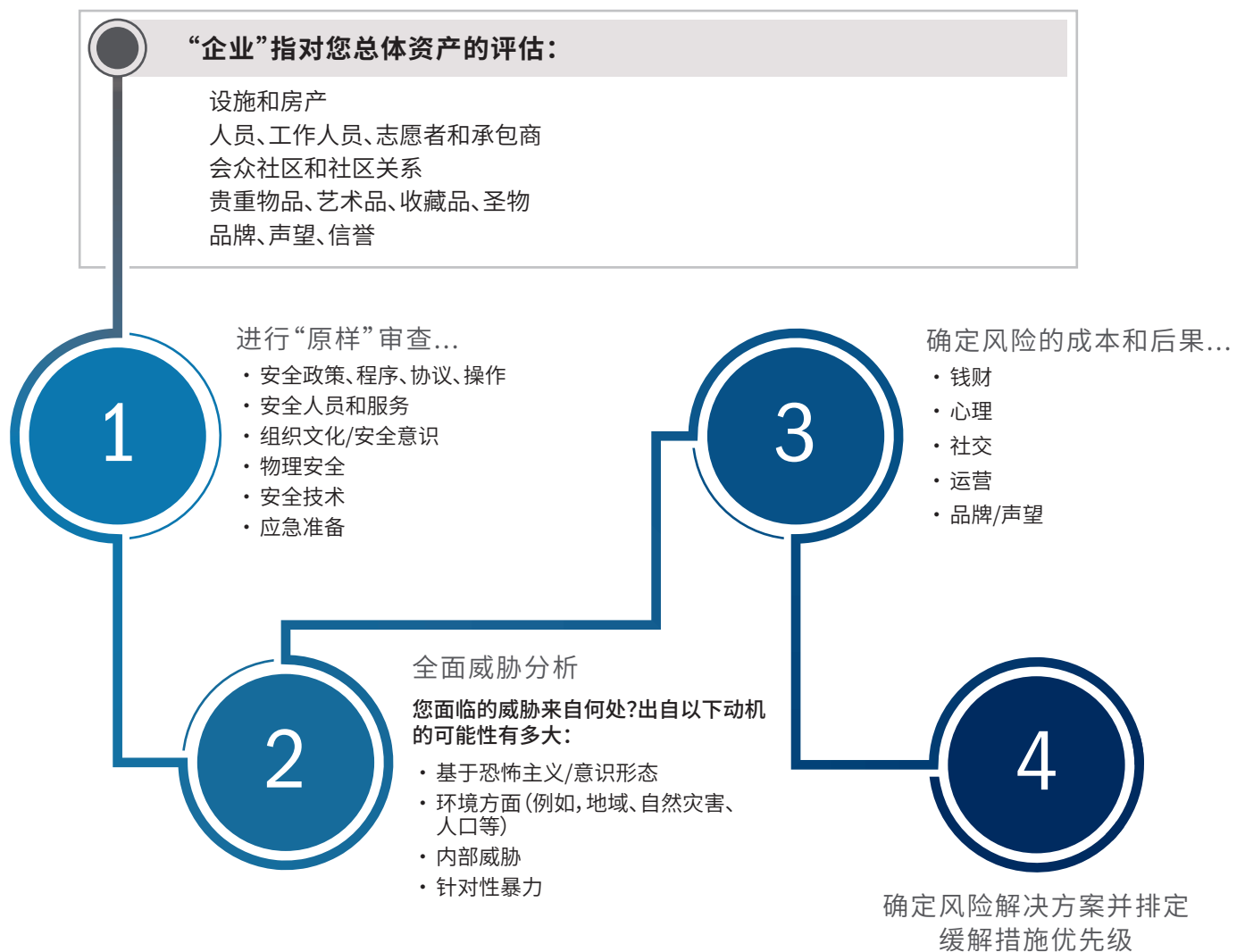
薄弱环节评估模型

要有高质量的评估,系统化的方法是关键。这一薄弱环节评估模型检查组织的职能领域,产生的结果可以在可行性、复杂性、预期效益、成本和资源可用性的背景下加以评估。

- ▶ 为了加强这一流程, CISA 开发出了宗教场所安全自我评估工具, 里面包含一组旨在揭示薄弱环节和改进领域的问题。此工具还可以当成模板, 根据组织的特定需求进行定制。还可以由 CISA PSA 或其他顾问为开展自我评估提供更多指导。

这种类型的评估通常包括通过采访关键人员和利益相关者来收集数据和信息, 进行现场检查和观察, 审查现有安全和培训计划等记录和材料, 以及查看当地犯罪统计等公共记录。

评估最重要的方面是记录您的流程和发现的结果, 以便可以复制流程本身, 并将数据用于制定安全策略。



运用薄弱环节评估模型的主要考虑事项

组织的资产

确定设施和房产

确定并描述您的设施：

- 确定您房产的每一栋建筑,如 HoW 主楼、教堂、教区、学校、操场、社区中心和停车场。
- 描述建筑物的数量、物理设计和施工(包括施工年份和类型)以及占地面积。
- 定义举行礼拜的类型和数量,以及在任何给定时间可能使用每栋建筑的时间表和会众数量。确定行政办公时间(工作日和时间)。列出所有可以帮助识别 HoW 房产的特征。

用外部、中间和内部边界定义房产。

- 外部边界通常包括停车设施和停车场、外部公共场地、人行道、游乐场和建筑物的实体立面。
- 中间边界是一个流动的区域,通常指“园区内”但在主要建筑之外的任何东西,包括人行道、门和墙壁等外部特征。
- 内部边界是任何内部空间,如门廊、礼拜区、行政办公室、社区室、礼堂和教室。
- 创建一份清单,列出所有外部、中间和内部边界元素。

确定资产和价值

确定任何需要保护的贵重物品以及更换的可能成本：

- 确定资产价值、保护资产(降低风险)的成本、更换资产的成本,以及资产损失时与组织声誉和生存相关的成本。
- 确定贵重物品,例如艺术品和圣物。
- 为贵重物品分派成本,可以简单评估为“高”、“中”或“低”。
- 对投资保护每项资产或降低其风险做出有依据的决策。



参见第 5 章了解物理安全指南和相关资源。

进行原样审核

审核管理惯例和与安全相关的规定

检查日常操作和相关的行政程序：

- 在来宾到访方面您有哪些措施？
 - › 您有固定的工作时间吗？
 - › 是否有定期上锁或开放的空间？
 - › 有没有在礼拜期间接待和筛查来宾的规定？有没有在非礼拜期间接待和筛查来宾的规定？
 - › 现有的规定是否一直在执行并且经常审核？
- 您是否有任何现成的应急措施或安全计划？它们是否涵盖了各种状况，如持枪乱射、应急准备、紧急疏散、威胁评估和学校安全？
- 您是否记录了所有管理流程、程序、政策、指令和操作手册？这些政策是否经常复查和更新？
- 谁来监督财务运营？包括供品和收藏品？您是否使用会计软件？是否有审计和监督制度？

1

检查人力资源实务

检查您的人力资源实务

- 您的组织是否使用合同安保人员（有没有武器）来保护 HoW 的活动和事件？如果有，他们的作用是什么？是否是因为当前社区有安全问题才雇用他们？安保人员是否符合所有州和地方的执照、培训和保险要求？
- 您是否与当地执法部门和/或在您管辖范围内有权力的急救人员建立了正式的关系和伙伴关系？您是否定期与他们会面，就安全和风险缓解优先事项交换信息并进行合作？



参见第 4 章
了解人力资源实
务的信息。

- 您遵循哪些就业前筛查规定?员工和志愿者是否接受背景调查,尤其是那些担任敏感职位的员工和志愿者,例如接触儿童、金钱、计算机系统或机密信息的员工和志愿人员?
- 目前的就业前筛查程序是否符合类似责任职位的实践标准?更多信息请参见 U.S. Equal Employment Opportunity Commission 的背景检查指南。



了解您的员工和组织文化

考虑您所在的社区对安全实践的态度:

- 您的会员是否普遍了解观察和报告可疑活动的最佳实践?例如,“If You See Something, Say Something®”。
- 组织领导人是否持续分享有关安全防护的信息?这是否为一个盲点?
- HoW 的职员和/或成员是否参加过紧急疏散、持枪乱射事件或其他重大事件的正式培训?
- 您是否有既定的流程来分享对可疑或不安活动的疑虑?
- HoW 成员和周围社区是否支持可能加大安保力度的安全策略?
- 会员非常关注哪些威胁或薄弱环节?
- 组织价值观和倡议(如支持弱势群体以及在社区提供食物、住所和社会支持)如何与安全措施理念保持一致?



参见第 4 章了解组织文化的信息。

全面威胁分析

评估威胁环境

建立对威胁环境的基本认知:

- 考虑组织的公众形象以及在社区和地区的知名度等因素。
 - 例如,了解与组织和/或 HoW 领导人相关的意识形态、社会或政治观点或信仰是否会引起高度关注和风险。



- 根据地点、成员、暴力历史和突出程度,分析各种威胁(例如,恐怖主义或基于意识形态的威胁)的发生概率。
 - › 不是所有的针对性暴力都是出于意识形态的。有些持枪乱射就是由家庭暴力、工作场所争议和精神健康危机引发的。
- 考虑位置和周边可能会如何影响您的威胁环境。例如,如果 HoW 位于经常成为公众关注焦点或暴力或故意破坏目标的组织旁边,则风险程度可能会增加。

要全面了解风险,首先要:

- 确定/列出每一类威胁或风险。
- 对发生概率和影响评级和排名(例如,低可能/高影响)。

确定与风险有关的成本和后果

了解与风险有关的成本和后果

进行风险分析,清晰确定与已识别风险相关的后果,包括:

- 有形损失,如金钱、财产和贵重物品;
- 可能扰乱 HoW 运营和业务连续性的社会、情感、人际和心理损害;或
- 对 HoW 在利益相关者和整个社区中的品牌、信誉或声誉的影响。

确定风险承受能力

讨论您所在社区的风险承受能力:

- 坦诚讨论对找出的每项风险的承受能力。与风险因素、风险承受能力和风险缓解相关的观点可能会不断演变;因此,评估风险和确定风险承受能力的过程应该是灵活的。

3

确定风险解决方案并排定缓解措施优先级

估计出现风险的可能性

考虑多种可能的情形与后果：

- 对于每种风险, 估计威胁发生的概率, 并将其与该风险相关的潜在成本和影响进行权衡。
 - › 可以使用更复杂的风险方法。这一评级将帮助为您的缓解策略排定优先级, 并为安全规划提供依据。
 - › 发生概率高和相关成本在的风险应在整体安全策略中列为高优先级。
- 缓解方案与风险可能存在以下关系：
 - › 缓解需求高
 - › 中等缓解需求
 - › 缓解需求低

4

总结

本章提供了一个框架, 用于设计和执行全面的薄弱环节评估。宗教场所可以定制这些工具和建议, 以评估组织资产和相关价值, 确定威胁环境, 分析风险和缓解方案, 并了解确定出的威胁有何后果。最后, 薄弱环节评估的广度和深度取决于资源、可行性和解决安全问题的紧迫性。评估结果应指导有关为具体措施排定优先次序的讨论, 这些措施会为组织的安全策略打下框架, 包括如何实施策略。





4

做好社区准备和防范

介绍

人员是宗教场所 (HoW) 要保护的最重要的资产,也是您防范可能威胁的最佳保护。本章的侧重点是组成 HoW 社区的人员,以及 HoW 在内部和更广泛的社区中运作方式相对简单的变化,这些变化可以改善您的整体安全态势。

人类行为、人际关系和社区价值观都在安全方面发挥着重要作用。有了合适的工具,人就可以成为找出可疑行为和活动的第一道防线。

本章列出了一些实施资本投入最小的政策和方案。下面的章节介绍了各个 HoW 可以独立实施的内部计划、在制定整体安全方案时需要考虑的特殊政策,以及与更广泛的社区建立联系以培养整体意识、准备能力和应变能力的方法。

最后,建立一种安全和负责任的文化,这是宗教场所准备和应对任何潜在针对性暴力行为的最佳方式之一。

您 HoW 社区的最佳实践

本章侧重宗教场所可以独立实施来改进其安全态势的常用方案。HoW 涉及众多人员,从神职人员、工作人员和志愿者到会众和访客,每个人都有自己的作用,如图 12 所示。

总的目标是创建一个环境,让负责人和会员在其中能对潜在的威胁或问题保持警觉,了解合适的上报渠道并知晓出现紧急情况时如何应对。常规训练和演习往往是最好的强化方式,它们挽救了许多生命。以下计划和举措将帮助您的社区做好应对多种突发情况的准备,它将宗教场所视为一个整体。

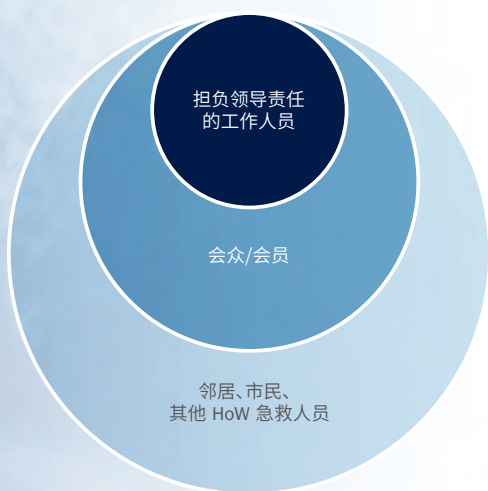


图 12. 宗教场所社区

宗教场所应该在安全计划中考虑到与组织打交道的所有人员。



建立安全文化

宗教场所可以通过维护基于共同价值观和安全目标体系的组织文化来提高其安全性。组织的领导层可以通过以下措施指导会员接受这些共同的价值观：

- 使安全目标与组织的核心价值观相一致，传送稳健的安全规定，让其成为社区共同的价值观；
- 让社区期望有安全的环境，积极促进沟通、保持透明度并提高响应能力；
- 建立清晰的信息共享流程，方便社区成员上报事件和/或让人担忧的行为，同时在评估报告后及时给出反馈，并保证保守机密；
- 提供内部培训，或利用外部资源进行培训，例如 Cybersecurity and Infrastructure Agency (CISA)、Protective Security Advisors (PSAs) 和 CISA 在线资源，并经常举办学习班；
- 在书面政策和指导方针中记录所有安全规定，并确保尽早并经常与社区共享。

认知和尽早识别

要应对或减轻威胁，您必须知晓威胁。让社区成员能尽早识别异常情况并报告是关键。宗教场所可以考虑开展一系列的活动并利用 Department of Homeland Security (DHS) 的大量资源为人员提供必要的工具，来侦测、威慑和减轻威胁：

- 与工作人员和会众分享 CISA 暴力之路视频和情况说明书。DHS 发布数项资源，帮助了解有暴力倾向人员的预警迹象。

暴力之路

一个人走上暴力之路的迹象包括：

- 不稳定、危险或攻击性的行为增多
- 对不公正或觉察到的不法行为有敌意
- 以有害方式使用毒品和酒精
- 边缘化或与朋友和同事疏远
- 工作表现发生变化
- 性格和/或家庭生活突然出现巨变
- 经济困难
- 待决民事或刑事诉讼
- 有威胁或报复计划的明显不满情绪

威胁识别

- ▶ 让工作人员熟悉各种指示潜在暴力行为的风险因素和征兆。
- ▶ 实施培训计划,提高对沟通或行为中早期预警信号的认识。
- ▶ 熟悉可疑活动报告 (SAR) 征兆和示例。
- ▶ 注意社区内的对话,尤其是当涉及到在线活动时。识别可疑活动并向有关当局报告,对于核实威胁的可信度和采取适当的缓解措施至关重要。

If You See Something, Say Something®

- ▶ 提高认识和加强早期识别是瓦解潜在威胁的最重要方式之一。“IF YOU SEE SOMETHING, SAY SOMETHING®” 活动(如图 13 所示)可以帮助向会员传达如何对可疑活动保持警觉,并通过合适的渠道上报。
- ▶ DHS 提供了一组产品来培训市民,包括“RECOGNIZE THE SIGNS”信息图表和可打印的便携式卡片,以及“IF YOU SEE SOMETHING, SAY SOMETHING® 公众认知视频”。

登录 “If You See Something, Say Something® ” 网站后还可以观看一组

- ▶ “TAKE THE CHALLENGE” 视频,并通过发现可疑活动测试他们的观察力。



图 13. If You See Something, Say Something® 的“5Ws”

这里的“5W”—何人、何事、何时、何地与何因—代表在联系当地执法机构或部门工作人员时要报告的重要信息。

图片来源: <https://www.dhs.gov/see-something-say-something>

问候的力量

CISA 建议宗教场所围绕“问候的力量”实施强有力的接待员方案，让它成为其整体安全策略的中坚。

如果有效使用，合适的用词会成为强大的工具。一句简单的“你好”就可以开启与陌生人的随意会话，帮助确定他们来访 HoW 的原因，以及他们是否会带来威胁。OHNO 方式—观察、问候、审视风险和得到帮助—协助会众观察和评估可疑活动，在必要时取得帮助：



观察： 识别可疑行为，例如拍摄设施或安全特征的照片/视频，使用一般人可能会感到威胁的辱骂性语言，或在没有合理解释的情况下在某个地点游荡。



问候： 与您在场所周围观察到的人互动。展现发现潜在威胁可以起到威慑和减轻风险的作用。



审视风险： 问自己您观察到的行为是否有威胁或可疑。个人的行为方式是否表明他们有正当理由在那里，还是让一般人起疑？



得到帮助 如果您认为某人存在真正的威胁，不要干预，从管理层或执法机构得到帮助。通过您所在 HoW 的合适渠道报告您的疑虑，如有紧急情况，拨打 9-1-1。

所有社区成员均可以进行问询，识别和报告可疑行为。有时只需要一句简单的“你好”就行。



练习问候的力量

微笑，进行目光接触，介绍自己，然后提问以下任何问题：

实践安全

“嗨，你好？”

“是专门来找人或者找东西吗？”

“今天我能帮什么忙吗？”

“我带你去找要找的人或者要去的地方。”

“我怎么帮你的忙？”

“如果需要帮忙就来这儿找我。”

“欢迎，是第一次来吗？”

跑开、躲藏、反击

有时,早期发现不足以防止事件发生;宗教场所应该培训其成员在发生袭击时如何应对。没有特定目标的袭击是无法预测的,并且会迅速演变。有些袭击者可能在警察到来前就在现场被制服了,所以人员必须在精神和身体两方面做好应对这一状况的准备。

- ▶ 如果出现武装袭击, CISA 鼓励市民跑开、躲藏,反击。

“跑开、躲藏,反击”涉及迅速评估形势,并确定在当时所在位置和情形下保护自己生命最合理的方式。在任何情况下,都可以选择以下三种选择中的一种:

1. 跑开: 如果有可进入的逃生通道,尝试疏散场所。

- › 记住逃生路线和计划。
- › 不要带随身物品。
- › 让人看到您的双手,并遵守警察给出的任何指示。

2. 躲藏: 如果疏散不可能,找一个袭击者不易找到的地方躲藏起来。

- › 躲藏在枪手视线之外的区域。
- › 封住藏身之地的入口并锁上门。
- › 将手机静音,也不要开启震动模式。
- › 保持安静。

3. 反击: 只有生命处于迫在眉睫的危险中时,才尝试瓦解和/或解除袭击者的行为,这是最后的手段。

- › 尽可能多地进行身体攻击。
- › 利用可当成武器的物品或向袭击者投掷东西。
- › 奋起反击...它能保护您的生命。

- ▶ HoW 负责人应与所有社区成员分享注意事项视频选项,确保每个人都熟知在发生潜在袭击时的不同选择。



跑开、躲藏、反击

在超过半数的 (n=13) 武装袭击案件 (n=20) 中,会众在袭击开始时选择跑开或躲藏。一些人能够从出口门逃生,而另一些人则躲在浴室、壁橱或家具下。在一个案例中,会众在听到外面的骚动后锁上了所有的外门,阻止袭击者进入。

在 45% (n=9) 的武装袭击案件中 (n=20),会众或目击者试图对付、瓦解或解除犯罪者的武装。一些受害者接受过标准的现场袭击培训,与袭击者对峙,其中一些人付出了生命的代价;其他人向袭击者投掷书、椅子或家具。许多这样的做法都对袭击者起到了拖延的作用,让其他人得以安全逃离。

心理健康和社会支持服务

一些有针对性的暴力事件源于心理健康危机,可能有迹象显示某人对自己和其他人构成危险。并非所有的心理健康危机都会导致暴力;然而, HoW 应该意识到个人处于危机中并可能走上暴力之路的迹象。

宗教场所在识别行为健康和阻止事态升级方面处于独特的地位。HoW 负责人经常是危机时期的第一联络点,在困难时期充当个人和家庭的决策咨询人或安抚人的角色。HoW 可以通过提高心理健康认知和让人们能更容易地寻求帮助来促进关爱文化。考虑以下加强社区防范能力的干预和援助选项:

- 了解有关心理健康的基本事实,包括某人可能需要帮助警示迹象。 ◀
- 对所在社区进行心理健康教育,并促成关于心理健康和身心健康主题的公开对话。
- 找出可能身处危机的社区成员,通过援助服务联系他们。
- 开发一个系统,找出最近未参加礼拜的会员并外联他们。
- 查看通过 U.S. Department of Health & Human Services 网站 [MENTALHEALTH.GOV](https://www.mentalhealth.gov) 为信仰领袖提供的最佳实践。 ◀
- 参加 U.S. Department of Health & Human Services Substance Abuse and Mental Health Services Administration (SAMHSA) 主办的化解年轻人中的暴力行为风险在线培训。 ◀
- 找出可以提供特殊支持的联络点,例如



减轻暴力强度

当一名身穿战术装备的武装男子威胁 Texas 州一座教堂的信徒时,牧师挺身而出站在枪手和会众之间。这位牧师利用他作为危机干预专家处理问题青年和罪犯的经验,通过与枪手交谈缓解了局势,枪手逃跑了,随后于次日被捕。

- 为员工、志愿者和感兴趣的成员提供减轻暴力强度培训计划,他们可能会用的上这一工具。
- 定期对封锁和持枪乱射应对程序进行培训。
- 就可疑活动对会员和工作人员进行教育,并明确建立报告机制。

心理健康、自杀预防、家庭暴力、虐待儿童、人口贩运和药物滥用。

- ▶ 使用 [FINDTREATMENT.GOV](https://www.findtreatment.gov) 是的 SAMHSA 找到附近的医疗点。
- ▶ 使用 SAMHSA 的行为健康治疗服务查找程序找到所在州的心理健康治疗机构。
- 考虑与社区中的专业提供方建立联系,这些提供方可以给出最佳实践和推荐。

特殊政策和长期规划

规划是制定整体安全策略过程的重要一环。实施了一些一般的最佳实践后,就可以开始对各种特定场景以及每种场景的潜在风险、威胁和结果进行规划了。本节重点介绍了一些更特殊政策,供 HoW 负责人和安全协调员在完善安全方案时加以考虑。

应急规划和事件响应

应急规划应该是任何安全方案的重要组成部分,包括确定您的组织将如何应对特定情况或事件。应急行动计划 (EAPs) 提供事件响应路线图,可以帮助 HoW 准备好应对任意数量的紧急情况。

- ▶ CISA 有一套资源用于事件管理规划和响应。创建 EAP 时,宗教场所可以考虑以下事项:
- ▶ • 查询 [Federal Emergency Management Agency \(FEMA\)](https://www.fema.gov) 为宗教场所制订高质量应急操作计划给出的指南(2013年6月),里面详细列出了为减少财产和生命损失可以在事件之前、期间和之后采取的措施。许多 HoW 还可以从 FEMA 提供的事件命令系统 (ICS) 培训中受益。
- ▶ • 确定您的 HoW 如何在出现任何紧急情况时继续运作。[READY.GOV](https://www.ready.gov) 在业务连续性套件中提供了一组产品,可以针对 HoW 的具体需求改编运用。
- ▶ • 使用 CISA 的持枪乱射应急计划指南和模板 [CDC](https://www.cdc.gov) 准备和响应中心的可定制模板制订自己的 EAP。

这些资源仅涵盖了全面整体安全策略所预计到的几个可能发生的情况。更多规划资源请参见附录 1。

安全小组和社区成员了解在出现袭击时如何应对是关键。实现这一目标的最佳方法是确保社区成员精通 EAP,并定期进行应急程序培训和演习。

人员安全实践

强有力的人员安全实践可以确保所有工作人员和志愿者都有良好的品格,并保持诚实守信的标准。与所有企业和组织一样,宗教场所应定期审核人员安全实践,以确保其符合标准商业实践,能对不断演变的威胁做出反应:

- **根据角色和职责列出敏感岗位。**
 - › 是否有业务运营需要对支持这些职能的人员进行更高级别的审查?
 - › 例如,考虑列出与儿童有联系、执行财务任务、管理和/或维护个人身份信息 (PII) 以及可以访问信息技术 (IT) 系统的人员。
- **列出应该或目前需要进行背景调查的岗位,并根据每个岗位的性质制定和实施自动取消就业资格的政策。**
 - › 是否对敏感岗位(员工、志愿者和承包商)进行岗前筛选?如果没有,需要哪些资源实施这一流程?
 - › 是否对这些岗位进行定期自我评估、正式审查和/或背景调查更新?

内部人员威胁

CISA 将内部人员定义为有权或曾经有权访问或了解组织资源的任何人,包括人员、设施、信息、设备、网络和系统。简单说,就是组织和社区成员所信任的人。内部人员威胁是指内部人员利用其访问权限或特殊了解,通过暴力、刺探、破坏、盗窃或网络手段伤害该组织的可能性。

将内部人员威胁缓解计划作为强有力的安全策略的一部分,可以让更多员工和社区成员具有安全意识;加强共同责任和资产保护的文化和;实现早期威胁识别;并保护组织的声誉。CISA 建议组织根据自己 HoW 的独有特性、其价值和您感觉风险最大的资源制订自己的内部人员威胁定义。

- ▶ 有效的内部人员威胁缓解方案:
 1. 根据宗教场所独有的任务、文化、重要资产和威胁情形**定制方案**。
 - ▶ 2. 按照 CISA 对识别和报告异常行为指南中所述, **建立报告和防范文化**,加强 HoW 对其人员身心健康的正向投入,同时提高整体应变能力和运营效率。
 - 3. **采用分层方法**,考虑 HoW 提供的多种岗位和职能。
 - 4. **应用“识别和报告”和“评估和响应”框架**检测、预防和减轻内部人员威胁(第 3 章中描述的薄弱环节评估流程的一部分)。
 - 5. **建立保护和援助文化**,来保护公民自由和保守机密。
 - 6. **协助组织提供一个安全、无威胁的环境**,识别并帮助可能构成威胁的个人,防止其行为造成伤害。
- ▶ 更多信息请参见 CISA 的内部人员威胁缓解资源。

报告程序

如果社区知道发现潜在的担忧或威胁该怎么办，并且要求领导层深思熟虑以确保问责制和明确定义适当的报告渠道，预防计划和“了解迹象”认知活动最有效。宗教场所应明确单核并传达报告标准和机制，并确保社区所有成员，特别是安全小组成员，熟悉组织的规定。

这些流程应包括可靠和及时的评估、通过适当渠道进行报告以及根据法律、政策和法规立即采取行动。有些情况下，报告可能在内部进行，涉及安全小组或 HoW 领导层。有些情况可能最好是将疑虑报告给执法机构或联邦机构。为确保会员和工作人员有必要的工具了解报告潜在威胁的内容、时机和方式，考虑以下事项：

- 参加可疑活动报告 (SAR) 私人领域安全培训，更好地了解如何报告可疑活动，以及如何将报告融入您的组织文化中。尽管是为政府机构编写的，但将可疑活动报告纳入机构运营的 10 种方式也为 HoW 提供了有用的指南。
- 让自己熟悉国家 SAR 方案 (NSI)，它为识别和报告可疑活动提供了标准化流程。
- 使用 “IF YOU SEE SOMETHING, SAY SOMETHING®” 活动和资源建立根据您的组织文化和安全策略定制的内部报告策略。
- 在组织安排人员担任可信的联系人，负责报告可疑活动。
 - › 确保这些人接受培训，了解所有安全规定。
 - › 向社区传达这一报告架构，以便他们了解在出现安全问题时的联系人。
- 建立接收、评估和处理社区成员报告的明确程序。
 - › 说明如何记录通知，处理保密问题，确定风险概率/影响，通知执法或心理健康官员 (如适用)，并根据需要进行进一步评估。
- 在工作人员和社区成员中分发 NSI 的信仰事件和 HoW 传单。

更大范围的社区参与

宗教场所在社区关系和凝聚力方面发挥着至关重要的作用,在努力改善 HoW 的安全态势时,这一作用会成为力量的源泉。有些 HoW 是公民团体和互助小组的聚会场所、活动场所、娱乐场所、选举投票场所和社区避难所。有些可能在努力与邻居和社区中的其他 HoW 建立有意义的联系。

扩大社区参与范围是一项重要的资产,可以帮助改进对潜在威胁的整体认知,提高抵御能力和建立外部伙伴关系,这些都会增强您的总体安全态势。

事件规划

鉴于 HoW 设计为对非成员敞开怀抱,某些类型的事件可能会加大风险。与社区参与和事件规划有关的安全注意事项应包括:

- 为在地界内举行的非礼拜活动制定和实施事件专用的安全实践。参见**群众集会:软目标和拥挤场所安全认知行动指南**中列出的最佳实践了解更多信息。◀
- 识别并持续评估在非礼拜活动期间的薄弱环节和潜在风险,视需要加强安全程序。
- 考虑是否纳入顾客筛选程序,以防止特殊事件期间设施中出现违禁物品,并纳入**顾客筛选最佳实践指南和公共场所行李搜查程序指南**中阐述的最佳实践。◀
- 用票据或签到表管理来宾和控制出席特殊事件的人数。
- 考虑联系当地执法合作伙伴或 CISA PSA,帮助制定宗教节日等重大活动的安全规划,或在您预计举行大型集会时提供帮助。

社区参与

基于社区的安全方法包括外联和认知活动。作为更广泛的安全策略的一部分，考虑促进社区防范的措施：

- 参与公众认知运动，教育社区，塑造公共话语，促进理解、宽容和接受。
- ▶ • 提名志愿者并选择社区成员参加高级面对面培训和研讨会，如**社区应急小组 (CERT)**、**持枪乱射事件应对准备**、**现场袭击和人质缓解**。
- 与当地执法部门、应急管理部门、附近企业和其他 HoW 一起进行例行的社区培训和演习。
- 赞助和推动社区学习基本急救和 CPR 课程。

社区中的信仰组织可以建立伙伴关系，以更好地共享信息、增强防范能力和改善安全性。考虑建立正式或非正式的结构和关系，并在社区内发展跨宗教团体，以汇集安全知识和资源：

- 与同一地域中的其他 HoW 互通有无。
 - › 考虑建立正式的跨宗教对话团体。
 - › 与 Department of Justice Community Relations Service 协调组织一个跨宗教社区合作伙伴**保护宗教场所论坛**。
- ▶ • 创建一个共享的、私人的社交媒体或其他交流空间，以便与您所在地区的其他 HoW 合作，集中信息共享。
 - › 识别来自对等沟通、共享信息、在线活动和社交媒体的可信威胁，并酌情向执法部门报告。
 - › 跟踪和报告近期在线出现的威胁。
- ▶ • 协调社区中的**防备预警活动**，鼓励社区做好准备和防范。

战略合作关系

要加强组织的安全策略, 培养和与维护与社区关键合作伙伴和急救人员的关系至关重要。强大的社区联盟有助于实现识别威胁、减轻风险和加强公共安全这些共同的目标。与当地执法机构和应急管理服务保持沟通也可以更好地做好准备, 还能更好地协调事件响应。

战略伙伴关系可以包括当地警察部门、消防部门、医疗应急服务以及地区和州组织。考虑用以下步骤来培养这些重要关系:

- 为自己的组织找到有急救人员监督的当地合作伙伴, 包括:
 - › 有管辖权的当地执法机构;
 - › 当地最近的消防部门和医疗急救单位;
 - › 最近的医院外伤中心; 和
 - › 附近的任何其他医疗急救服务, 包括心理健康资源。
- 通过定期外联与当地执法部门和其他急救人员建立关系。
 - › 巡查房产并分享建筑计划, 确保熟悉该房产。如果房产和地表有重大变化, 用最新版本跟进。
 - › 查看安全规定并开展和/或参加正式和非正式的培训。
 - › 使用社区社交活动在急救人员和其服务的邻居之间建立联系。



专业联络伙伴关系

- 对您 HoW 的响应时间是多少?
- 他们巡视过你们的设施吗?
- 他们过去有没有到过您的 HoW? 如果有, 出于什么原因?
- 是否向他们提供了您所在设施的建筑结构图纸/平面图?
- 他们有没有在您的 HoW 举办过培训? 如果邀请, 他们是否会给出培训?
- 他们可以提供哪些公共安全课程和培训?

- ▶ • 使用 [READY.GOV TOOL](#) 找出您当地/地区的应急管理组织。联系最近的办事处并订阅警报(如果有)。
- ▶ • 找到距您最近的 [CISA 地区办事处](#) 并与 [CISA PSA](#) 建立联系。查看 [CISA 的 PSA 情况说明书](#), 更多了解通过此区域方案提供的服务。
- ▶ • 如果您的 [HoW](#) 位于联邦设施内或其周边, 联系 [DHS 联邦保护服务](#)。
- 与联邦执法部门建立对话, 了解规划和培训资源, 更好地了解可疑活动报告和事件响应。
- 让您的区域融合中心参与威胁监测和调查。

总结

人类行为、人际关系和社区价值观对安全预防、准备和缓解方案的有效性有着巨大的影响。培养关爱和共担责任文化的 [HoW](#) 能够很好地应对当前和新出现的威胁, 这里提供的工具可以帮助您找到最适合您的 [HoW](#) 及其服务的更广泛社区需求的方法。



5

保护您的设施

介绍

任何安全保障方案均旨在尽早识别出潜在风险,确定最佳行动计划,并在风险导致人身伤害或财产损失之前将其降至最低或瓦解。如第 4 章所述,您可以通过改变自己宗教场所 (HoW) 内的政策、实践和行为,用最少的资本投资来解决许多问题。但是,有些薄弱环节可能需要对您设施的结构和场地做出重大更改。本章概述了改进物理安全的一些选项及其潜在影响。

热情的环境并不等于毫无防范。

为界定不同的薄弱环节和责任领域,请考虑您的建筑划分为三个不同的区域:建筑外部、建筑中间部分和建筑内部。有效的安全策略必须涵盖 HoW 的全部责任,从建筑的最外侧到最内侧的圣所。最安全的规划从建筑外部开始,然后延伸到中间和建筑内部。每个区域的安全特征应充分整合,并考虑各区域之间相互关联的薄弱环节和风险。这一区域系统还为部署安全方案(例如交通管理或接待员)提供了框架。

本章中介绍的缓解方案包括组织交通模式、种植树篱、安装围栏和照明、闭路电视 (CCTV) 视频监控以及完善建筑物出入控制。这些选项共同支持一种分层方法,它包括所有已找出的物理安全薄弱环节和风险,并考虑一系列潜在威胁场景。

无论是从成本看还是出于不愿“强化”或“加固”一座以开放、热情为宗旨的建筑,增加或升级物理安全的前景似乎都令人望而生畏。The Cybersecurity and Infrastructure Security Agency (CISA) 强调有许多选项可以考虑,其中一些要求最低量的资本投资。许多 HoW 还有资格获得联邦和州拨款,以抵消改进成本, HoW 负责人和安全小组可以利用 CISA 和本指南中列出的其他联邦机构提供的其他免费资源,制定适合自己需求的物理安全改进计划。

拨款资助

为了应对针对宗教场所的袭击,有些州和地方政府已通过立法,资助进行安全改进。确保核实适用您所在 HoW 的资助选项。

在联邦层面, Department of Homeland Security (DHS)、Federal Emergency Management Agency (FEMA) 和国会正在加大拨款力度,协助 HoWs 改善安全状况。FEMA 制订了非营利组织安全拨款方案,该计划为“符合条件的非营利组织提供了加强物理安全和其他活动的资助,这些组织面临着恐怖袭击的高风险,并且所在城区属于 DHS 的 UASI 拨款方案指定的城市地区安全倡议管辖区”。国家行政机构可能也属于合格的非营利组织。FEMA Grant Programs Directorate 的工作人员还会与 HoW 合作制订应急准备和预算指南,以帮助 HoW 规划安全改进事宜。要了解更多信息,请访问 www.fema.gov/grants。



外部边界

确定您 HoW 的总责任区(院落边界的最外侧)是规划流程的关键一环,具体视不同的宗教场所而定。最重要的是根据尺寸、现有保护特征(如障碍物、围栏、大门和照明)以及观察到的风险(如有)来定义该外部边界。

外部边界通常是弥补薄弱环节或减轻攻击的第一个机会,每个 HoW 占地区都自己独特的挑战和情况。有些区域可能包含体育比赛或户外活动用的大型场地。有些可能包含地面停车场,其中不一定有围栏、照明、监控或其他安全特征。一些 HoW 可能有街道停车场,而其他 HoW 可能使用不隶属于该组织的多层停车设施。

一旦安全规划小组定义了外部边界,就可以识别薄弱环节,确定可能的缓解方案,并根据概率、影响和成本确定解决方案的优先级。宗教场所,特别是那些考虑新建或翻新的宗教场所,可能会在“通过环境设计预防犯罪”(CPTED)的概念中找到有用的启迪,该概念侧重于建筑环境如何塑造人类行为。即使是具有成本效益的微小解决方案,例如改变景观来改善视线或使用混凝土花圃和路桩来控制通道都可以产生重大影响,同时最大限度地提高投资回报。



用设计求安全

FEMA 发布了详细的指导意见,说明现场和建筑设计如何帮助减轻袭击的风险和破坏。

现场和城市安全设计:防御潜在恐怖袭击指南(2007)
风险管理系列

缓解针对建筑物的潜在恐怖袭击的参考手册(2011)
建筑物和基础设施保护系列

安全实践



车辆袭击威胁是外部边界需要特殊考虑的事项。一般来说, 车辆袭击分为两类: 车辆撞击和车载简易爆炸装置 (VBIEDs)。这两类车辆袭击最可能发生在外部边界附近。虽然第 1 章中介绍的研究没有指出任何用于袭击宗教场所的 VBIED, 案件研究中仍包含了两起车辆撞击袭击。管理交通模式, 让志愿者、接待员、安保人员或执法人员指挥交通, 尤其是在高峰时段, 可以帮助识别可疑活动。安装障碍物, 如混凝土花圃或路桩, 也可以形成一个“隔离”区, 来帮助保护会众。

想要更改建筑外部时, 考虑以下某些选项:

建筑外部选项

安全特征	类型	益处和资源
------	----	-------

照明

- | | |
|---|---|
| <ul style="list-style-type: none"> · 太阳能 · 定时路灯 | <ul style="list-style-type: none"> · 阻止潜在的袭击者和/或入侵者。 · 照亮所有区域, 使工作人员和会众能够安全地穿过停车场和地面。 |
|---|---|

沿建筑外部和整个场地战略性地放置维护得当的照明设施, 这一做法可以阻止未经授权的进入, 加强工作人员和会众的安全。既有具备夜间照明功能的太阳能灯, 也有由定时器或开关控制的标准路灯。

围栏和大门

- | | |
|--|---|
| <ul style="list-style-type: none"> · 视觉障碍物 · 实体障碍物 · 景观设计 | <ul style="list-style-type: none"> · 不许与 HoW 无关的个人进入场地和设施。 · 围栏造型还可以具备美学效果。 |
|--|---|

边界围栏和大门具有不同的风格和功能, 有的用于区分院落边界的简单视觉屏障, 有的用于防止或限制进入场地。围栏和大门也可以连接建筑物出入控制、照明和视频监控系统。

CCTV (视频监控)

- | | |
|---|--|
| <ul style="list-style-type: none"> · 仅限录像 · 实时监控, 但没有响应功能 · 实时监控, 且有响应功能 | <ul style="list-style-type: none"> · 支持监测可疑行为且提供早期警告和提示。 · 阻止入侵者 · 清除盲点。 · 规划注意事项: 复杂的协同袭击 |
|---|--|

在安装 CCTV 监控系统之前, 请考虑该技术是否与总体安全策略、需求和容量相符。CCTV 有多种实施方式, 从无监控的录像系统, 到由签约安全机构实时监控且与事件响应计划集成的系统。

建筑外部选项

安全特征	类型	益处和资源
交通管理		
	<ul style="list-style-type: none">· 大门/路桩· 通道/标志· 来宾停车· 接待员、志愿者、执法机构	<ul style="list-style-type: none">· 定义人员和车辆流动。· 支持早期预警功能, 并实现非侵入式视频监控。· CISA 车辆撞击行动指南· CISA VBIED 检测课程情况说明书
<p>受控交通管理流程通过大门、路桩、交通锥、标志或指挥交通的工作人员限制交通流量, 保护所有社区成员免受事故和车辆袭击。应使用反光背心或制服明确标识参与此流程的人员。在某些情形下, 当地的执法机构可以给出协助。</p>		
应急通信		
	<ul style="list-style-type: none">· 紧急呼叫站 (紧急警报箱)	<ul style="list-style-type: none">· 能够在出现紧急情况下联系 HoW 安全部门和/或执法机构。· 将大型设施中远离主楼区域的风险降至最低。
<p>找出院落中远离主楼且需要紧急警报箱的区域, 例如远处的停车场、步行道或祈祷花园。任何硬件均需要经常维护和测试。</p>		
景观		
	<ul style="list-style-type: none">· 清除灌木· 安装功能	<ul style="list-style-type: none">· 去除杂草丛生的灌木, 提高能见度· 清除所有可燃材料
<p>确保对院落和场地进行维护。清除任何妨碍视线或存在潜在危险的灌木或景观特征。考虑添加景观特征, 如大型花圃, 这可能有助于引导交通或阻止未经授权的出入。</p>		

建筑中间

建筑中间是一个流动的区域, 通常指“园区内”但在主要建筑之外的任何区域。例如, 主楼的墙壁和外门将被视为建筑中间的一部分, 操场或野餐区等附属建筑或空间也是如此。其建筑, 如学校、教区或现场住宅, 被视为建筑中间的一部分, 但其安全情况需要与 HoW 主楼分开考虑。第 1 章中的几个案件研究揭示了与建筑中间安全相关的潜在薄弱环节, 袭击者或是穿过该区域, 或是从此区域发起袭击。在薄弱环节评估期间, 应详细描述建筑中间, 以便不熟悉现场的人 (如急救人员或外部安全顾问) 能够快速看到里面的情况, 提高应急响应行动的速度。

建筑中间通常会出现多种类型的薄弱环节和威胁，它需要全方位的安全计划来解决这些复杂的情况。

野餐区和/或操场是需要特殊注意的建筑中间，需要额外加以考虑。由于儿童经常去这些区域，所以建立出入控制和持续进行监控是头等大事，例如，安装 CCTV 摄像头和/或配备志愿者和安保人员。如果可能，通过围栏或物理障碍物控制此区域的进出，防止未经授权进入。

确定建筑中间安保所需的功能并排定优先次序时，考虑以下选项：

建筑中间选项

安全特征	类型	益处和资源
门		
<ul style="list-style-type: none">· 木料、玻璃或金属· 抗冲击或防爆		<ul style="list-style-type: none">· 上锁的门可以阻止入侵者，并有助于控制人群流动和进出。· 训练有素的接待员安排在有利的位置上，可以帮助识别可疑行为。
<p>确定入口点的数量以及何时使用。它们由哪种材料构成（木料、金属还是玻璃）？它们是如何锁紧的（锁和钥匙还是门禁卡）？它们有警报装置吗？考虑在紧急情况下，袭击者是否可以挡住或锁住门以防止逃跑。</p>		
窗户		
<ul style="list-style-type: none">· 有警报· 用门锁锁紧		<ul style="list-style-type: none">· 锁上后，窗户可以阻挡入侵者。· 出现紧急情况时，还可以从窗户逃走。
<p>窗户可能是未经授权的入口，尤其是在地面上，但如果门口受到阻碍，也可以当成紧急出口。考虑它们是否可以上锁并锁紧，但在需要也可以轻松打开？玻璃上是否有纤维保护材料？它们有警报装置吗？</p>		
CCTV（视频监控）		
<ul style="list-style-type: none">· 仅限录像· 实时监控，但没有响应功能· 实时监控，且有响应功能		<ul style="list-style-type: none">· 支持监控可疑行为和提醒，包括早期报警功能。· 阻止入侵者· 清除盲点。
<p>需要覆盖的区域可能包括外部门口入口、交通繁忙的室外人行道或盲点。如前面“外部边界 CCTV”一节中所述，建筑中间的 CCTV 可以没有监控，也可以用响应计划进行监控。</p>		
门禁		
<ul style="list-style-type: none">· 标准门锁和钥匙· 电子门禁		<ul style="list-style-type: none">· 仅允许有授权的人员进入，可以与 HoW 时间表搭配使用。
<p>选项包括基本的门锁和钥匙控制、使用门禁卡或遥控钥匙的更复杂的电子应用程序，以及与时间表和指定出入级别集成的软件程序。</p>		

建筑中间选项

安全特征	类型	益处和资源
入侵警报		
· 安装在门窗上		· 快速提醒安保人员、执法部门或其他紧急服务部门有入侵者。
考虑成本与投资回报、组织的安全需求和与院落和设施相配的功能,例如运动传感器。		
应急发电机		
· 以天然气为燃料		· 支持紧急服务,如信息技术 (IT)、火灾探测、门禁、CCTV 系统和其他互联的安全功能。
· 以柴油为燃料		
· 最低运行寿命: 24 小时		
应急发电机确保关键系统在紧急情况下保持运行,如疏散照明、电梯、供暖、通风和空调 (HVAC) 以及新鲜空气回流。停电可能会造成混乱和痛苦,袭击者可以利用这些混乱和痛苦造成更多的损害和/或伤害。新鲜空气回流应高于地面,以防止干扰 HVAC 系统。露出的基础设施应加上盖,用上锁的金属盖保护,并用 CCTV 监控。		
景观		
· 清除灌木		· 去除杂草丛生的灌木,提高能见度。
· 安装功能		· 清除所有可燃材料。
确保对院落和场地进行维护。清除任何妨碍视线或存在潜在危险的灌木或景观特征。考虑添加景观特征,如大型花圃,这可能有助于引导交通或阻止未经授权的出入。		

建筑内部

圣所或建筑内部毫无疑问是最重要的保护区域,因此里面有最重要的资产:人员。在大多数情况下,这将是主楼,但其他建筑,如学校、教区或住宅,也有自己的建筑内部区域,可能包括儿童室、行政办公室、祈祷室或其他公共区域。

在第 1 章中探讨的 37 起针对性暴力行为中,有 43% (n=16) 发生在内部边界或圣所中。建筑内部的人群最密集,这个区域的袭击通常的伤亡最大。为保护人员,建筑内部区域需要最高级别的检查、控制和监护。

侧重建筑内部的安全措施应尽可能详细。安全小组的成员应有明确定义的岗位和责任。所有会众成员应知晓第 4 章中给出的基本安全培训,并了解紧急疏散或现场袭击场景的规定。要了解学校和托儿所设施安全措施的特殊注意事项,参见第 6 章。

建筑内部安全通常包括以下内容:

建筑内部选项

安全特征	类型	益处和资源
------	----	-------

圣所

- 礼拜主区域
- 会众最多
- 持枪乱射应急准备方案
- 对会众进行紧急程序培训
- CISA 持枪乱射应急准备

圣所是另一个最重要的保护区域,应该是安全规划流程的重点。事件管理和应急行动计划应围绕圣所和在那里提供的礼拜展开。

接待/来宾管理

- 人员是 HoW 最宝贵的安全资产
- 问候的力量
- 识别可疑活动培训
- 快速识别可疑活动、邮件或电话
- 帮助控制 HoW 来宾的流动并管理进出。
- CISA 问候的力量资源

考虑建立来宾管理系统。对于有行政或接待人员的 HoW, 提供适当的培训并实施详细的安全程序, 包括授权/预先筛选的来宾名单、通知和筛选、处理可疑邮件/电话以及报告可疑活动。确保所有来宾均知晓太平门的位置。

门禁

- 标准门锁和钥匙
- 电子门禁
- 仅允许有授权的人员进入, 可以与 HoW 时间表搭配使用。

选项包括基本的门锁和钥匙控制、使用门禁卡或遥控钥匙的更复杂的电子应用程序, 以及与时间表和指定出入级别集成的软件程序。

儿童室/学校

请参见第 6 章

避难室

- 无窗房间, 有带锁的门或其他安全的内部空间
- 在发生持枪乱射事件时提供安全的躲藏空间
- 缓解针对建筑物的潜在恐怖袭击的参考手册
- 风险评估: 缓解针对建筑物的潜在恐怖袭击的方法指南

确定在出现恶劣天气和/或事件(例如, 持枪乱射)时的避难所或“安全室”。这些位置应该是没有窗户且门上锁的房间。工作人员和来宾应该知道这些房间的位置并了解它们的用途。培训可以帮助工作人员做好准备, 在紧急情况下引导会员前往这些地点。避难所用于应对恶劣天气, 如龙卷风或吸入外部空气可能构成威胁的危险物质事件。

建筑内部选项

安全特征	类型	益处和资源
急救/AED		
	<ul style="list-style-type: none">· 商店购买· 专业服务	<ul style="list-style-type: none">· 工作人员和会众有必要的工具在出现紧急情况时迅速做出反应。· 在帮助到来之前您就是帮助
<p>急救包和自动体外除颤器 (AEDs) 等救生设备应存放在有明确标记的位置, 并定期检查, 以确保用品库存充足且未过期。应检查和维护 AED 以保障其功能正常。与供应品公司签约来提供此服务。</p>		
火灾报警和灭火系统		
	<ul style="list-style-type: none">· 商店购买· 专业服务	<ul style="list-style-type: none">· 快速提醒安保人员、消防部门或其他紧急服务部门有入侵者。
<p>火灾和烟雾报警器以及灭火系统应符合州、县和市标准。大多数建筑在获得占用许可之前都要接受应急系统检查。每个 HoW 均应该有功能正常且符合标准的烟雾和火灾探测器。这些报警器应每年进行一次检查, 以确保其功能无误。</p> <p>灭火器应放置在所有建筑物的各处, 并做好标记, 方便在紧急情况下使用。根据当地标准的要求, 也应该对其进行检查和维护。</p>		

总结

将宗教场所职责区域划分为建筑外部、中间和内部区域提供了一个有用的框架, 用于组织安全方案和考虑提高物理安全可能需要的升级或修改。薄弱环节评估帮助顺利识别薄弱环节和风险, 并优先考虑您认为必要的任何更改, 它的效率和性价比都是最高的。





6

托儿所和学校安全注意事项

介绍

为儿童提供一个安全的学习和发展空间是全国社区的核心价值观。学校和托儿所中心特别容易受到针对性暴力的袭击，这导致许多学校近年来实施了强有力的安全方案。对于 K-12 学校、暑期项目、托儿所设施、宗教学习和放学后项目，以及与宗教场所相关的周末看护项目，学校暴力的威胁更大。确保儿童和教育工作者的安全环境至关重要，宗教场所 (HoWs) 应优先考虑学校或托儿所设施的安全规划，同时考虑所有相关的薄弱环节和风险。此处提供的指南以 Department

- ▶ of Homeland Security (DHS) 制订的学校安全基本要素为基础，网站 SchoolSafety.gov 有详细信息。

设施评估

首先评估学校或托儿所设施附属社区的场地和需求，例如学生和教职员工的数量、出口和入口的数量以及房间的数量。在此基础上定制更准确的评估和安全计划，有效保卫这些设施。为了顺利完成这一流程，Cybersecurity and Infrastructure Security Agency (CISA) 建议使用无成本评估，包括 CISA 的 K-12 指南和评估工具，U.S. Department of Education 管理的学校准备和应急管理 (REMS) 网站评估应用程序。

- ▶ 指南和评估工具，U.S. Department of Education 管理的学校准备和应急管理 (REMS) 网站评估应用程序。

儿童保育和教育不存在万能的方法。不过，政府和私营部门提供了许多资源，帮助工作人员根据当地法规制定和实施学校和托儿所中心的安全措施。其中包括有关学校安全政策、物理安全、学校氛围、行为健康技术、培训和资助机会的资源。CISA Protective Security Advisors (PSAs) 也可以提供专业的现场评估。

- ▶ SchoolSafety.gov 向教育设施提供工具，为儿童和教育工作者维护一个安全的环境。资源是在整个准备过程中组织的：**防止、保护和缓解、应对和复原**。学校和托儿所中心的工作人员可以进行自我评估，以获得个性化的行动计划和下一步行动，并获得一系列宝贵的资源、培训和相应的拨款资助。

程序和规定

对于防止和应对威胁而言，一组合适的程序和规定是关键。考虑制订学校安全行动计划和应急操作计划 (EOP)，并分派专人负责安全，以防范针对学校或托儿所设施的一系列威胁。安全措施应兼顾物理和行为安全注意事项，以及机构的政策。完整的规划流程应包括以下步骤：

- 量身定制学校安全行动计划，确定帮助保障学校安全的重要后续步骤。
- 分析当前政策中的薄弱环节，如信息缺失、缺乏指导和/或过时的做法，并相互参照此列表与最佳做法，以找出可能需要新程序或改进的领域。
- 学习在线课程制订应急操作计划 (EOPS) K-12 101，更多了解如何创建有效 EOP 和实施计划。
- 使用跨部门的高质量学校应急操作计划制订指南建立基本准则，并遵循六个步骤的规划流程。
- 采用 DHS 的恢复策略资源清单协助创建强大的恢复计划。

考虑纳入安全计划的主要政策包括：

- 儿童接送政策
- 儿童监护人或对儿童负有法律责任的人 (父母除外) 的政策
- 监督暂停和实施足够物理安全措施的政策
- 家庭纠纷规定
- 对院落内或周边来宾及可疑人员的规定
- 对院落内另一建筑内的现场事件的规定

物理安全

学校和托儿所的物理安全注意事项包括更多的薄弱环节,例如操场、教室和指定的接送区域。宗教场所应使物理安全规划与第 5 章中提供的更广泛的建议保持一致,并针对与这些独特元素相关的风险进行量身定制。HoW 应考虑以下额外的防范措施:

- ▶ 在 CISA PSA 和 SchoolSafety.gov 资源的帮助下评估当前学校/托儿所当前的物理安全态势,或使用 DHS 学校安全调查找出物理功能和设备的差距,并确定更新操作的优先级别。
- ▶ 使用 Readiness and Emergency Management for Schools (REMS) 场地评估安全移动应用程序进行安全评估,收到定制的待办列表。
- ▶ 按照安全学校合作伙伴联盟- K-12 学校安保指南中所述,在各个边界内采取措施加强安全。
- ▶ 考虑 SchoolSafety.gov 建议的物理安全策略。

学校氛围

为学生提供一系列的社交、情感和行为支持系统,培养强大的情商,让学生以更有意义的方式与同龄人和教育工作者相互沟通。这些系统可以改善学校氛围,防止暴力,同时培养健康的心理,并使学生能够在出现可疑或危险情况时敢于表达。2019 年 U.S. Secret Service (USSS) 报告指出,80% 的学校袭击者之前有过引发关注公共安全和袭击者安全的行为。¹ 向 HoW 工作人员和学生提供安全的环境,鼓励每个人报告引发关注的行为,这样能通过早期干预帮助减少出现暴力的几率。这种方法要想成功,要求学校不但优先重视学校氛围,还要提供对可用报告机制的指南。HoW 可以参考以下资源来改善附属学校和托儿所中心的整体学校氛围:

- ▶ 查看指导原则:改善学校氛围指南,了解建立积极向上学校氛围的三大准则。
- ▶ 使用学校氛围改进行动指南评估改进学校氛围的五项关键行动。每个均提供了行动条目、注意事项和要考虑的问题。
- ▶ 访问 SchoolSafety.gov 上的学校氛围资源来评估其他主题资源和可用的拨款选项。

1 National Threat Assessment Center, Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence (2019), U.S. Secret Service, U.S. Department of Homeland Security, https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.pdf.

行为健康

如第 4 章所述, 在学生以及教职员中提倡行为健康是防止学校暴力的重要一步。心理和行为健康问题通常还会影响学生的社交和学业成功。例如, 2017 年的一项调查发现, 12-18 岁的学生中约有 20% 遇到过欺凌。² 欺凌是一种常见的现象, 会严重影响身心健康, 也是产生某些学校暴力案件的一个因素。通过利用现有资源帮助识别引人关注的行为, 并努力改善学生的身心健康, HoW 可以帮助在其学校和托儿所中心创造更安全的环境。³ 考虑运用以下步骤和资源, 在有威胁或引人关注的行为发展为暴力前加以识别和解决:

- **开展行为威胁评估, 以评估潜在的可疑活动并加强对行为健康的支持。**
 - › 由专门的多学科小组进行此项评估, 成员包括来自多个学科有资质的专家, 并由其提供支持。该小组至少应包括一名学校行政人员、一名心理健康顾问和一名学校资源官。
 - › 一旦培训完成并确立了明确的角色, 小组应为行为威胁评估流程制定全面的书面计划、政策和程序, 包括评估报告的威胁和引人关注行为的流程。
 - › 小组应不断审查报告的威胁和其他引发关注的行为, 以确定干预和缓解的领域。
 - › 通过 USSS 使用威胁评估模型加强学校安全找到详细的指南和资源, 指导组建小组、开展威胁评估, 以及为学校创建后续政策和程序。 ◀
- **完成学校健康评估和表现评估系统的学校心理健康档案, 大概了解现有的心理健康服务和系统。这一概述将有助于确定差距, 并有助于国家层面对学校心理健康系统进行跟踪。** ◀
- **实施欺凌预防能力评估和变革计划, 以确定学校在七个领域预防欺凌的能力。** ◀
 - › 评估后, 利用“欺凌预防组合方案”来查看有证据的欺凌预防驱动因素, 以提高当前的能力。

2 “Facts About Bullying.” StopBullying.gov, U.S. Department of Health and Human Services, 2020 年 8 月 12 日, <https://www.stopbullying.gov/resources/facts#stats>。

3 “Bullying and Cyberbullying,” SchoolSafety.gov, U.S. Department of Homeland Security, <https://www.schoolsafety.gov/prevent/bullying-and-cyberbullying>。

培训

培训和演练对于学校和托儿所人员能够帮助预防和应对紧急情况的环境至关重要。学生应接受相关培训,了解在出现有害天气或持枪乱射这类事件期间保持安全的最佳做法。了解政策、角色和程序有助于更好地做出响应,缓解产生负面后果的风险。HoW 可以考虑以下策略来培训学校工作人员,并确保政策、流程和程序不过时:

1. 按照以下步骤,就学校 EOP 和实施计划的各个方面对学校行政人员和工作人员进行培训:
 - A. 就 EOP 中的角色和责任培训工作人员。
 - B. 指定工作人员协调和实施 EOP 练习。
 - C. 与所有工作人员一起进行年度演习,以实践 EOP 程序。如果合适,包括社区合作伙伴。
 - D. 开展培训练习来相应更新 EOP,同时评估当前计划。⁴
- ▶ 2. 应请求提交 REMS 培训申请,以接受关于制订 EOP 和防范策略的面对面培训。
- ▶ 3. 使用 DHS 校园防范方案演习入门包,让学生和教职工自行完成桌面演习。
- ▶ 4. 运用国土安全演习和评估计划指南中的原则来制定、执行和评估额外的演习计划。应根据组织对学校安全活动和政策的优先级别来使用此指南。
- ▶ 5. 查看 SchoolSafety.gov 上提供的培训、演习和练习来了解更多策略和资源。

⁴ “Training, Exercises, and Drills.” SchoolSafety.gov, U.S. Department of Homeland Security, <https://www.schoolsafety.gov/respond-and-recover/training-exercises-and-drills>

资助资源

在向其 State Awarding Agency (SAA) 或直接向拨款实体申请后, 非营利 HoW 学校可能有资格得到以下所述的拨款:

- **非营利组织安全拨款方案**
 - › 支持加强面临高风险恐怖袭击的非营利组织的安保。
- **杜绝学校暴力方案 (SVPP)**
 - › 通过循证性质的学校安全方案帮助资助方所辖的学校改善安全状况。
- **安全学校方案所用的停止学校暴力技术和威胁评估解决方案**
 - › 通过建立学校威胁评估小组, 使用匿名报告与学校暴力有关的可疑活动的技术, 以及通过建立和加强州立学校安全中心, 更努力地减少暴力犯罪。
- **学校暴力应急响应 (SERV)**
 - › 资助当地教育机构 (LEA) 和高等教育机构 (IHE) 的短期和长期教育相关服务, 以支持在发生破坏学习环境的暴力或创伤事件后的恢复。
- **E 级方案**
 - › 为公立学校和图书馆提供具有成本效益的技术, 以改善网络基础设施并为未来的教育需求做好准备。

要了解更多与拨款机会有关的信息, 请访问 SchoolSafety.gov。

总结

宗教场所下辖的学校和托儿所与全国各地类似的设施有许多相同的特点和薄弱环节, 由于信仰关系, 更是多了一层风险。对于拥有此类设施的 HoW, 在制定和实施强有力的安全政策以保护学生和教师并保护他们的学习环境时, 应始终知晓这些独特的挑战和威胁。





7

网络安全

介绍

互联网使得可以用前所未有的方式联系到信仰社区。许多宗教场所 (HoW) 都在利用技术为自己服务, 例如实时流传输服务和通过在线门户建立社区。这种技术带来了极大的便利, 但也为新出现的威胁打开了大门。网络黑客在不断寻找新的目标和可以利用的薄弱环节, 而 HoW 也不能幸免。

基于信仰的组织由于其访问和存储的信息类型而容易受到网络攻击; 由于它们的规模和被认为缺乏网络保护, 它们被视为容易攻击的目标。在正常运作时, 信仰组织从会众、捐赠者和员工那里收集和存储大量个人和财务信息。这类个人身份信息 (PII) 可用于实施身份盗窃、从银行帐户盗窃和确定其他攻击目标。除了诈骗钱财的网络黑客, 犯罪者还可能出于意识形态原因将 HoW 定为目标。无论哪种情况, 网络攻击都可能以难以克服的方式损害 HoW 的声誉, 干扰该机构的整体使命。

网络袭击类型

尽管恶意网络黑客可以使用多种方法, 但本报告中进行的事件分析显示, HoW 特别容易受到以下类型的攻击:

金融欺诈

就像任何其他经手钱财和组织一样, HoW 也面临金融欺诈的风险。许多信仰组织现在使用在线或移动平台收取捐款, 为欺诈带来了新的薄弱环节和机会。金融欺诈可能与多种险恶的方法有关, 包括由网络钓鱼和恶意软件引起的网络入侵。

网络安全应被视为安全和应急计划的新成员。

勒索软件

越来越多的恶意网络黑客使用勒索软件来攻击医院和市政机构这类软目标, 这种软件旨在要求付费才能访问电脑系统或数据。在这些类型的攻击中, 网络黑客得到易受攻击网络的访问权, 加密文件, 然后索要付款。

网站篡改

另一个潜在的弱点是网站篡改, 即网络黑客进入网络或网络服务器, 用自己的信息更改或替换网站内容。这些袭击通常以仇恨的语言或图像为特征, 试图引起恐惧, 破坏社区建立宗教间对话的努力。信仰社区正在受到越来越多的网站篡改攻击。

建立网络攻击应对准备文化

要减小网络风险, 需要有多层次的整体方法, 与化解物理威胁所用的方法非常相似。HoW 必须将网络防范纳入任何涉及机构和会众准备的安全计划中。要管控网络风险, HoW 需要在整个组织推行基本网络规范和数据保护, 制订出强有力的安全实务, 打造网络攻击应对准备文化。

作为国家的风险顾问和负责保护国家网络空间的主要民事机构, Cybersecurity and Infrastructure Agency (CISA) 负责建立国家防御网络攻击的壁垒。CISA 专门开发并向信仰组织提供多项资源, 帮助 HoW 缓解各种网络威胁。各种规模的 HoW 都可以使用下面列出的资源和提示, 开始做出改变, 得到更安全的在线形象。

CISA 提供直接的网络安全专业知识, 并建议与地区 CISA CYBER SECURITY ADVISORS (CSAs) 建立联系, 以加强网络安全准备、风险缓解和事件响应能力。



建立网络攻击应对准备文化

6 网络攻击应对准备文化的要素

实践
安全
攻击

您自己	推动网络安全策略、投资和文化
您的工作人员	培养安全意识和警惕性
您的系统	保护重大资产和应用程序
您的周边环境	确保只有属于您数字工作场所的人才拥有访问权
您的数据	制作备份, 避免丢失运营必需的重要信息
危机应对措施	减轻损害程度, 迅速恢复正常运营

更多信息参见: CISA 的网络要素

CISA CYBERSECURITY ADVISORS (CSAs)

何人?	区域 CISA 工作人员, 提供援助和一线支持, 帮助利益相关者做好准备并保护其免受网络安全威胁。
何地?	遍布于整个美国的十个 CISA 区域。
何事?	通过伙伴关系和直接援助活动, 如现场会议、为工作组创造条件以及事件协调和支持, 让私营部门实体和州、地方、部落和领土 (SLTT) 政府参与进来。
何因?	提高网络安全准备、风险缓解和事件响应能力, 创建公众与 Department of Homeland Security (DHS) 网络方案沟通的渠道。

网络清洁环境

组织必须从头建立网络攻击应对准备文化, 这就要求改变思维方式。网络清洁环境需要建立基本级别的网络安全, 提高工作人员、志愿者和会众的风险意识, 以加强抵御能力, 减轻潜在入侵或攻击的影响。随着我们的文化继续依赖于网络技术及其带来的好处, 网络安全变得越来越重要, 并且是各种规模和位于各个地点组织的重要考虑因素。

HoW 应对关键网络安全概念的认知视为优先事项, 并采纳行业最佳实践, 大多数互联网服务提供商都有能力帮助解决许多常见的薄弱环节。除了网络安全资源路线图中所列的步骤, 信仰组织还可以使用几种常识性的方法来建立网络安全文化:

- ▶ 参见 CISA 的网络要素了解组织网络攻击应对准备文化的关键信息。
- ▶ 始终了解最新的安全信息, 如有可能, 启用自动更新。
 - ▶ 了解软件补丁和软件更新
- ▶ 订阅国家网络认知系统 (NCAS) 来接收网络安全警报、分析报告、公告或提示。
- ▶ 经常备份重要文件和数据。
 - ▶ 需要额外备份和保护的重要文件可能包括: 财务记录; 会众名单、地址和 PII; 房产记录; 员工和志愿者档案; 在线捐赠记录等。

- 对可疑电子邮件始终保持警惕, 打开附件或链接时要加倍小心(小心处理电子邮件附件)。
- 如果可行, 对网站管理员帐户启用双因素身份验证 (2FA)。
- 了解手机存在的风险, 做出调整来保障与 HoW 关联的移动设备的安全。
- 为员工制定基本的安全惯例和政策, 例如要求使用强密码, 并制定适当的互联网使用指南, 详细说明违反公司网络安全政策的处罚。坚持运用这些政策。
- 建立处理和保护会众和捐赠者信息及其他重要数据的行为规则。考虑通过限制访问权限、密码保护的文件和安装软件来保护网站与捐赠平台。
- 在所有电脑上安装防病毒软件并定期更新。

在线安全

互联网使信仰组织更容易与会员和潜在新会员建立联系, 而社交媒体则提供了保持联系和分享最新消息的有效方式。不过, 访问的便利性和非正式性也使这些平台对想窃取现成信息的恶意黑客具有了吸引力。虽然许多网站都是良性的, 但社交媒体平台已经被用来传播恶意代码。同样, 发布在社交媒体上的个人信息可能被用于进行社交工程攻击, 或用于为个人攻击做准备, 例如利用礼拜时间表或计划。即使没有技术高超的黑客, 网络平台也会被那些试图欺凌或恐吓的人利用。

实践安全

选择可靠的密码

正确做法

- 使用允许的最长密码
- 使用符号和数字
- 每个帐户使用不同的密码

错误做法:

- 使用可以在字典中找到的词
- 根据个人信息使用密码
- 分享自己的密码



采用基本级别的安全和认知可以让 HoW 继续安全地在线连接。以下资源可以帮助您保持在线联系的安全：

- ▶ • 实施常用的在线隐私最佳实践措施，如在线隐私提示表中所述。
- ▶ • 查看在社交网站上保持安全和社交媒体网络安全提示表了解与社交媒体有关的威胁。
- ▶ • 参见在线发布信息指南并监测在设施网站或社交媒体帐户发布的信息，包括礼拜和活动时间表。考虑每周而不是每月发布时间表，或者将时间表限制在成员门户上。
- 注意通过电子邮件发送给会众的内容。通讯录保持最新状态，确保您只向需要信息的当前成员发送电子邮件。
- 做出调整，优先考虑社交安全。
- 网络欺凌的严重程度各不相同，可能表明有更严重行为的倾向。了解网络欺凌的基础知识并参阅处理网络欺凌了解保护您社区的信息。
- ▶ • 了解社交工程引发的风险，实施避免社交工程和网络钓鱼攻击中列出的程序。

安全实践和认知

除了所有个人和组织可以采用的基本最佳实践外，HoW 还可以考虑实施更先进的措施，以提高对潜在网络事件的抵御能力。一个强有力的网络安全方案包括的活动会专注于网络事件应对规划、培训关键利益相关者以及制定报告规定来识别可疑活动。制订有效的网络安全方案既需要知晓战术，又要有新的思维方式。HoW 应考虑以下事项：

- ▶ • 参见如何识别和防止网络犯罪提示卡和 CISA 的报告网络事件网站，确定报告网络事件的起点和方法，内部向安全方案经理报告，外部向相关当局报告。
- 与其他信仰机构交流他们所用的保护措施。确保分享您得到的信息，以向他们提供帮助。
- ▶ • 订阅 US-CERT 月度公告，了解有关网络安全在线研讨会和讨论、新文献和最佳实践方面的信息。
- ▶ • 自行开展 CISA 网络防范审核 (CRR)，评量现有的安全措施，找出需要改进的领域。
- ▶ • 知晓在出现危机时如何沟通与谁沟通，包括向 CISA 报告网络攻击和事件及上报相关当局。

- 创建详细的数据和物理资产存储表并定期更新。
 - › 其中包括硬件和软件的制造商、型号、序列号和支持信息。如果是软件，要有安装和运行的具体版本。
 - › 了解数据和技术的存储位置和有权访问这两项内容的人员。
- 使用收费漏洞扫描服务或 CISA 的免费静态互联网协议 (IP) 扫描在您的网站上进行漏洞测试, 检测已知的漏洞和弱点。
- 参见 CISA 洞察见解: 修复互联网可访问系统的漏洞了解更多信息。定期备份数据, 避免丢失运营必需的重要信息。 ◀
 - › 考虑多种数据备份方式, 包括自动备份数据的解决方案。
 - › 维护联机和脱机两种备份方式, 脱机备份不是永久连接其所备份的电脑和网络。这种做法可以降低备份损坏的风险。
- 定义组织中预期的行为, 在工作人员中创建安全文化。要求遵守最终用户协议和企业网络安全政策。
- 与基于信仰的合作伙伴和地方政府机构建立信任关系网, 分享威胁情况和及时获取网络威胁信息。
- 参加 CISA 主办的区域会议, 这些会议的重点是不断演变的网络威胁管理需求和供多个领域和区域使用的社区资源。
- 使用 CISA 的弹性网络桌面演习包(CTEP), 根据自己组织的具体情况生成和定制桌面网络演习。 ◀
- 组织应确定其透露敏感个人身份识别信息的风险。一旦确定了这一风险, 他们应遵循行业最佳实践来防止信息泄露。 ◀
- 制订全面的网络事件响应计划并对工作人员进行相应培训, 这些计划侧重能够通过已知的准确备份恢复系统、网络和数据。
 - › 确保该计划得到组织高级领导层的正式批准, 从而保证计划得到接受。
 - › 定期测试您的事件响应计划, 以确保组织的每个部门都知道如何应对基本和大规模的网络安全事件。

瓦解具体的威胁

网络攻击有多种形式,每一种都相应需要特定的响应。幸运的是,这些反制措施经常重叠,是创建强大的网络清洁环境和应急准备文化的重要组成部分。

恶意软件和病毒

恶意软件和病毒是恶意软件程序,旨在破坏电脑或移动设备的完整性,让攻击者能够监视您的活动或窃取您的数据。要保护自己和组织免受恶意软件和网络入侵的攻击,有几个重要的注意事项:

- 为工作人员讲解可能感染设备的各类恶意软件以及保护此类设备的最佳实践。阅读 **CISA 恶意软件提示卡**。
- 所有安全软件、web 浏览器和操作系统均为最新版本,以防止攻击者利用已知漏洞
- 不要单击电子邮件或在线发帖中的可疑链接。
- 使用安全软件扫描 U 盘 (USB) 和其他可能被病毒和恶意软件感染的外部设备。

网络钓鱼攻击

网络钓鱼攻击使用电子邮件或恶意网站感染机器或收集个人和财务数据。网络钓鱼电子邮件可能貌似来自真实的机构或网站,可能索要个人信息。如果用户回复了索要的信息或单击了提供的链接,攻击者随后即可访问帐户。几个关键的注意事项可以帮助您防止网络钓鱼:

- ▶ 让您的工作人员熟悉 **CISA 网络钓鱼提示卡**中介绍的最佳实践和潜在网络钓鱼电子邮件示例。
- 不要单击电子邮件中的超链接。如果可能,在搜索栏中输入 URL。

威胁中心



识别网络钓鱼攻击

什么是网络钓鱼?

1. 电子邮件是否貌似来自真实的机构,但进一步检查却发现稍有不同(例如, .net 而不是 .com, 缺少字母等)
2. 电子邮件是否要求通过电子邮件或单击链接提供个人信息?
3. 电子邮件是否恳求你迅速采取行动以避免严重后果?
4. 将鼠标悬停在 web 链接上,它是否指向与文字不相关的网站?

如有疑问,将其扔掉: 如果它看似可疑,将其删除!

- 要小心那些提供天花乱坠的东西或敦促迅速采取行动的电子邮件。
- 不要在电子邮件中透露个人或财务信息,也不要回复请求该信息的电子邮件,包括通过电子邮件发送的链接。
- 注意可疑电子邮件中提供的电子邮件地址或网站 URL。恶意网站和帐户可能看起来与合法网站和电子邮件相同,但可能拼写不同或使用其他域。
- 如果不清楚电子邮件请求是否合法,请尝试直接联系公司或在线搜索公司,但不要使用电子邮件中提供的信息!

勒索软件

勒索软件攻击使用恶意软件以勒索为目的拒绝访问系统或数据。将用户锁定在数据或系统之外后,恶意网络攻击者将系统或数据作为要挟,直到支付赎金。勒索软件攻击经常通过钓鱼电子邮件和不安全的应用程序锁定最终用户目标。预防是抵御勒索软件最有效的措施,因此务必考虑以下几种预防措施:

- ▶ • 让工作人员熟悉 CISA 的勒索软件套件,包括“战胜勒索软件”网络研讨会和防范勒索软件安全提示。
- 打开电子邮件附件时要小心,尤其是当附件是压缩文件或 ZIP 文件时。
- ▶ • 要了解保护组织网络和应对潜在勒索软件的信息,参见勒索软件指南,它是以客户为中心的一站式资源,有最佳实践和预防、保护和应对勒索软件攻击的方法。
- 实施认知和培训方案。由于最终用户是目标,因此员工和其他有权访问网络的人应该知晓勒索软件的威胁及其传播方式。
- 确保经常用最新的安全补丁更新所有应用程序和操作系统。
- 安装并定期更新防病毒软件、防火墙和电子邮件过滤器,以减少恶意网络流量。
- ▶ • 配置防火墙阻止访问已知的恶意 IP 地址,这些地址可以在 NCAS 警报和分析产品中找到。

网站篡改

如果攻击者取得了面向公众网站的控制权,则会发生网站篡改。过去几年, HoW 遇到越来越多的网站篡改攻击。这些类型的攻击通常以令人不安的图像和语言为特征,目的是向目标社区灌输恐惧,损害网站及其所有者的声誉。攻击网站可能威胁到网站的信誉,以及其中包含的信息的机密性。对于信仰组织来说,这可能会造成极大的破坏和尴尬。HoW 可以采取几个重要的步骤来防范对网站的网络攻击:

- ▶ • 让工作人员熟悉网络安全的基础知识。
- 查看您组织的网站托管服务商提供的服务,并与他们联系,讨论根据所提供的服务实施安全措施。
- 更改域注册商和域名系统 (DNS) 提供的所有默认用户名和密码,因为这些用户名和密码通常在互联网上很容易获得,并且可能在攻击中使用。
- 定期更新系统上可以更改组织 DNS 记录或网站的所有帐户的密码。
- ▶ • 定期审查所有域的注册商和 DNS 记录。参见 [CISA 网络洞察见解:缓解 DNS 基础架构篡改](#) 了解更多信息。
- 强制对所有授权用户和网站管理员实施多因素身份验证 (MFA)。
- 启用日志记录并定期审核网站日志,以检测安全事件或不正当访问。应进一步调查异常或可疑的访问情况。
- ▶ • 定期扫描和修补重大的高风险漏洞。参见 [CISA 网络洞察见解:修复互联网可访问系统的漏洞](#) 了解更多信息。

总结

HoW 对于网络攻击来说不是牢不可破的。观察网络攻击事件并报告所有发现的异常情况,这是保护自己组织的重要方式。CISA 提供了几种广泛使用的服务,帮助各种规模的组织为网络事件做好准备和给出响应:

- ▶ • 如果您的组织遇到了事件,请考虑通过 [CISA 的安全报告工具或事件报告系统](#) 报告任何网络钓鱼企图、恶意软件或找到的漏洞。
- CISA 分析恶意软件、网络钓鱼消息以及网站或软件漏洞,以提供可操作的信息,帮助公民在未来更好地保护自己。
- CISA 鼓励您报告您认为符合事件或网络钓鱼攻击标准的任何活动。CISA 的政策是对您组织的所有特定信息保密,除非您允许发布此类信息。

建立网络攻击应对准备文化要求转换网络安全思路,并对基本的网络清洁环境进行重点投资。了解网络安全的基本知识,纳入简单的最佳实践,这些做法可以大幅提升您的设施防范破坏性网络攻击的能力。应该对员工和志愿者进行这些最佳实践和程序的培训,并让他们了解在网络危机期间如何识别和应对可疑的活动。网络安全应被视为安全和应急计划的新成员。

8

总结和总体结论

针对宗教场所 (HoWs) 的攻击从统计角度看数量并不多,但却是对美国人民真正的威胁,是 Department of Homeland Security (DHS) 的头等要务。Cybersecurity and Infrastructure Security Agency (CISA) 以国家风险顾问的身份编制了本指南,以帮助宗教场所和信仰组织制定全面的安全策略,帮助保护生命和财产。

在本安全指南中, CISA 分析了十年来针对宗教场所的攻击,为前几章中概述的企业范围的安全建议提供了背景。回顾的案件研究是宗教场所每天面临的广泛威胁的示例。从持枪乱射事件或爆炸等物理袭击到无形的网络攻击,宗教场所应在其安全实践对这些都保持高度警惕。

要减少可能的袭击,最好的办法就是采取整体安全方法。这要求在整个组织中为制订安全决策、规划和实施程序与功能分派清晰的岗位和责任。应该根据宗教场所的具体需求和优先事项量身定制强大的安全计划。

要制订和实施可靠的安全实践惯例, CISA 建议考虑以下选项:

- 建立多层次安全计划,为制订和实施安全措施确定明确的岗位和责任。
- 制定应急行动计划、业务连续性计划和事件响应计划,并与安全小组就这些计划进行良好的沟通和演练,取得完整的理解。
- 评估薄弱环节以了解宗教场所的风险,并从中优先实施任何后续安全措施。

- 建立关爱的组织文化, 为所有成员和来宾提供适当的支持, 并通过先前确定的渠道报告可信的威胁, 让社区做好应对准备, 提高防范能力。
- 采取物理安全措施, 监控和保护周边的外部、中部和内部, 同时尊重宗教场所每个区域的用途。
- 围绕儿童保育、托儿所以及学校实施安全措施, 重点保障儿童的安全。
- 实施网络安全最佳实践, 以保护重要信息并防止潜在的网络袭击。

这些安全选项不是万能的, 但全面的安全方法是在出现袭击时保护人员和财产的最佳解决方案。HoW 应根据其独特的安全需求定制这些知识, 同时确保保持固有的开放和热情的价值观。

展望

CISA 将继续与信仰组织 (FBO) 合作, 了解此类袭击的现象, 并就如何减轻风险提供指导。展望未来, CISA 清楚指出需要做更多的调研, 并采取某些切实的重要步骤来为针对 HoW 的暴力行为制订常用定义、开发统一的跟踪和报告系统来为未来的分析和安全规划提供依据, 并继续联合全国的 HoW 以更好地分享资源、观点和解决方案。



附录 1: 宗教场所综合资源

本节中的资源指南综合了此安全指南中提供的所有资源,按章节加以整理。这份清单并不详尽,但提供了有用的信息,可以根据风险和优先级为任何宗教场所 (HoW) 的安全计划量身定制。

类别

资源

第 1 章: 介绍

DHS, Strategic Framework for Countering Terrorism and Targeted Violence (打击恐怖主义和针对性暴力战略框架)

<https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence>

FBI, Hate Crime Tracker (仇恨犯罪跟踪器)

<https://www.fbi.gov/services/cjis/ucr/hate-crime>

第 2 章: 确定整体安全方法

DHS Hometown Security Report Series for Houses of Worship (DHS 本地宗教场所安全报告系列)

<https://www.cisa.gov/publication/houses-worship-hometown-security-report-series-may-2017>

DHS Guide for Developing High Quality Emergency Action Plans for Houses of Worship (DHS 宗教场所高质量应急行动计划制订指南)

<https://www.fema.gov/emergency-managers/individuals-communities/faith-preparedness>

CISA Active Shooter Emergency Action Plan Template and Guide (CISA 持枪乱射应急行动计划模板和指南)

<https://www.cisa.gov/publication/active-shooter-emergency-action-plan-guide>

CISA Active Shooter Emergency Action Plan Video (CISA 持枪乱射应急行动计划视频)

<https://www.cisa.gov/active-shooter-emergency-action-plan-video>

CISA Faith Based Organizations - Houses of Worship Security Resources (CISA 信仰组织 - 宗教场所安全资源)

<https://www.cisa.gov/faith-based-organizations-houses-worship>

CDC Emergency Action Plan Template (CDC 应急行动计划模板)

<https://www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.pdf>

FEMA Producing Emergency Plan Guidelines (FEMA 应急计划制作指南)

<https://training.fema.gov/hiedu/docs/cgo/week%203%20-%20producing%20emergency%20plans.pdf>

FEMA Center for Domestic Preparedness (FEMA 本地准备中心)

<https://cdp.dhs.gov/>

FEMA Emergency Kit Checklist (FEMA 应急工具箱检查表)

<https://www.fema.gov/media-library-data/1553273223562-797451b5cb0bee8d35d3e4e85e3830d6/Checklist.pdf>

FEMA Faith-Based Community Preparedness (FEMA 信仰社区准备)

<https://www.fema.gov/emergency-managers/individuals-communities/faith-preparedness>

American Red Cross First Aid Checklist (美国红十字会急救检查表)

<https://www.redcross.org/get-help/how-to-prepare-for-emergencies/anatomy-of-a-first-aid-kit.html>

应急准备

CDC Crisis Communication Plan (CDC 危机沟通计划)
https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf

CISA Active Shooter Preparedness (CISA 持枪乱射应急准备)
<https://www.cisa.gov/active-shooter-preparedness>

CISA Active Shooter Workshops (CISA 持枪乱射事件研讨会)
<https://www.cisa.gov/active-shooter-workshop-participant>

CISA Run-Hide-Fight Video (CISA 跑开-躲藏-反击视频)
<https://www.youtube.com/watch?v=W2Vqt5KqAQ&feature=youtu.be>

CISA Active Shooter Preparedness Video (CISA 持枪乱射应急准备视频)
<https://www.cisa.gov/options-consideration-active-shooter-preparedness-video>

CISA Active Shooter Training for First Responders (CISA 持枪乱射事件急救人员培训)
<https://www.cisa.gov/first-responder>

应急操作

Ready.gov Active Shooter Resources (持枪乱射事件资源)
<https://www.ready.gov/active-shooter>

Ready.gov Training Resources (培训资源)
<https://www.ready.gov/training-0>

Ready.gov “You Are the Help Until Help Arrives” (在帮助到来之前您就是帮助)
<https://community.fema.gov/until-help-arrives>

“Stop The Bleed” (止血)
<https://www.stopthebleed.org/training>

DHS Improvised Explosive Device Training (DHS 简易爆炸装置培训)
<https://cdp.dhs.gov/training/course/AWR-337>

CISA Vehicle Attack Mitigation (CISA 车辆袭击缓解措施)
<https://www.cisa.gov/first-responder>

CISA Insider Threat Training (CISA 内部人员威胁培训)
<https://www.cisa.gov/training-awareness>

Ready.gov Business Continuity Planning Suite (业务连续性规划套件)
<https://www.ready.gov/business-continuity-planning-suite>

CISA Active Shooter Recovery Guide (CISA 持枪乱射恢复指南)
<https://www.cisa.gov/publication/active-shooter-recovery-guide>

CISA Emergency Services Sector Continuity Planning Suite (CISA 应急服务部门连续性规划套件)
<https://www.cisa.gov/emergency-services-sector-continuity-planning-suite>

业务连续性

CISA Hometown Security: Connect, Plan, Train, Report (CISA 本土安全:联系、规划、培训、报告)
<https://www.cisa.gov/connect-plan-train-report>

FEMA National Continuity Programs (FEMA 国家连续性方案)
<https://www.fema.gov/media-library/assets/documents/89510>

DOJ Helping Victims of Mass Violence Toolkit (DOJ 帮助大规模暴力受害者工具包)
<https://www.ovc.gov/pubs/mvt-toolkit/recovery.html>

第 3 章: 开展全面薄弱环节评估

CISA PSAs
<https://www.cisa.gov/protective-security-advisors>

CISA House of Worship Security Self-Assessment (CISA 宗教场所安全自我评估)
<https://www.cisa.gov/publication/houses-worship-security-self-assessment>

EEOC Background Check Guidance (EEOC 背景检查指南)
<https://www.eeoc.gov/background-checks>

第 4 章：做好社区准备和防范

CISA Pathway to Violence Video (CISA 暴力之路视频)

<https://www.cisa.gov/pathway-violence-video>

CISA Pathway to Violence Fact Sheet (CISA 暴力之路情况说明书)

<https://www.cisa.gov/publication/pathway-violence-fact-sheet>

DHS If You See Something, Say Something® 信息图表

<https://www.dhs.gov/see-something-say-something/recognize-the-signs>

DHS If You See Something, Say Something® 便携卡

<https://www.dhs.gov/see-something-say-something/campaign-materials>

DHS Risk Factors and Indicators (DHS 风险因素和征兆)

<https://www.dhs.gov/publication/risk-factors-and-targeted-violence-and-terrorism-prevention>

CISA Insider Threat: Recognize and Report Anomalous Behavior (CISA 内部人员威胁: 识别和报告异常行为)

<https://www.cisa.gov/recognize-and-report>

DHS If You See Something, Say Something® : Take the Challenge (接受挑战)

<https://www.dhs.gov/see-something-say-something/take-challenge>

DHS Suspicious Activity Reporting (SAR) Indicators and Examples (DHS 可疑活动报告 (SAR) 指标和示例)

<https://www.dhs.gov/publication/suspicious-activity-reporting-indicators-and-examples>

DHS Nationwide SAR Initiative (NSI) Training: Private Sector Security (DHS 全国 SAR 活动 (NSI) 培训: 私人领域安全)

<https://www.dhs.gov/course/nsi-training-private-sector-security>

DHS How to Integrate Suspicious Activity Reporting Into Your Agency's Operations (DHS 如何将可疑活动报告纳入机构运营)

<https://www.dhs.gov/publication/10-ways-integrate-sar-your-agency-s-operations>

DHS Nationwide SAR Initiative (NSI): Safety for Faith-Based Events and Houses of Worship (DHS 全国 SAR 活动 (NSI): 信仰事件和宗教场所安全)

<https://www.dhs.gov/publication/safety-faith-based-events-and-houses-worship-nsi-awareness-flyer>

FBI Field Office Contact Information (FBI 外勤办事处联系信息)

<https://www.fbi.gov/contact-us/field-offices>

FBI Tip Form (FBI 提示表)

<https://tips.fbi.gov/>

FEMA Incident Command System (ICS) Resource Center (FEMA 事件命令系统 (ICS) 资源中心)

<https://training.fema.gov/emiweb/is/icsresource/>

CISA Mass Gatherings: Security Awareness for Soft Targets and Crowded Places (CISA 群众集会: 软目标和拥挤场所安全认知)

<https://www.cisa.gov/publication/active-assailant-security-resources>

CISA Patron Screening Best Practice Guide (CISA 顾客筛选最佳实践指南)

<https://www.cisa.gov/publication/patron-screening-guide>

CISA Public Venue Bag Search Procedures Guide (CISA 公共场所行李搜查程序指南)

<https://www.cisa.gov/publication/public-venue-bag-search-guide>

Ready.gov 社区应急小组 (CERT)

<https://www.ready.gov/cert>

DOJ Protecting Places of Worship Forum (DOJ 宗教场所保护论坛)

<https://www.justice.gov/crs/our-work/facilitation/protecting-places-of-worship>

Ready.gov "Prepareathon"

<https://www.ready.gov/prepareathon>

CISA Regional Resiliency Assessment Program (RRAP) (CISA 区域防范评估方案 (RRAP))

<https://www.cisa.gov/regional-resiliency-assessment-program>

威胁管理

社区参与和社区关系

	Ready.gov Local Emergency Management Information (当地应急管理信息) https://www.ready.gov/local
	Tool to Identify Nearest CISA Regions (找到距离最近的 CISA 区域工具) https://www.cisa.gov/cisa-regional-offices
专业联络伙伴关系	CISA Protective Security Advisor (PSA) Program Fact Sheet (CISA 保护安全顾问 (PSA) 方案情况说明书) https://www.cisa.gov/publication/psa-fact-sheet
	DHS Federal Protective Service (DHS 联邦保护服务) https://www.dhs.gov/topic/federal-protective-service
	MentalHealth.gov “What is Mental Health (什么是心理健康) ?” https://www.mentalhealth.gov/basics/what-is-mental-health
心理健康和社会支持服务	MentalHealth.gov Talk About Mental Health: For Community and Faith Leaders (讨论心理健康: 社区和信仰负责人) https://www.mentalhealth.gov/talk/faith-community-leaders
	SAMHSA Addressing Risk of Violent Behavior in Youth (SAMHSA 化解年轻人中的暴力行为风险) https://www.samhsa.gov/sites/default/files/addressing-youth-violence.pdf
	SAMHSA FindTreatment.gov https://www.findtreatment.gov/
	SAMHSA Behavioral Health Treatment Services Locator (SAMHSA 行为健康治疗服务查找程序) https://findtreatment.samhsa.gov/locator/stateagencies.html#.XurGoG5Fwgo

第 5 章: 保护您的设施

拨款	FEMA Nonprofit Security Grants Program (FEMA 非营利组织安全拨款方案) https://www.fema.gov/grants/preparedness/nonprofit-security
	FEMA Types of Grants (FEMA 拨款类型) https://www.fema.gov/grants
用设计求安全	FEMA Site and Urban Design For Security (FEMA 现场和城市安全设计) https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf
	FEMA Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 缓解针对建筑物的潜在恐怖袭击的参考手册) https://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf
	FEMA Planning Considerations: Complex Coordinated Attacks (FEMA 规划注意事项: 复杂的协同袭击) https://www.fema.gov/media-library-data/1532550673102-c4846f270150682decba99b37524ca6/Planning_Considerations-Complex_Coordinated_Terrorist_Attacks.pdf
威胁管理	CISA Vehicle Ramming Action Guide (CISA 车辆撞击行动指南) https://www.cisa.gov/publication/active-assailant-security-resources
	CISA TRIPwire: Vehicle Born IED Identification Guide: Parked Vehicles (车载 IED 识别指南: 停放的车辆) https://www.fbiic.gov/public/2008/oct/DHSVehicleBorneIEDIdentificationGuideParkedVehicles.pdf
	Office of the Director of National Intelligence (DNI): First Responder Toolbox (国家情报总监办公室 (DNI): 急救人员工具箱) https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox
	CISA Security and Resiliency Guide (CISA 安全和防范指南) https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience
	DHS Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (DHS 缓解针对建筑物的潜在恐怖袭击的参考手册) https://www.dhs.gov/science-and-technology/bips-06fema-426-reference-manual-mitigate-potential-terrorist-attacks-against
	FEMA Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 风险评估: 缓解针对建筑物的潜在恐怖袭击) https://www.fema.gov/media-library-data/20130726-1524-20490-7395/fema452_01_05.pdf

第 6 章: 托儿所和学校安全注意事项

类别	资源
一般资源	DHS SchoolSafety.gov https://www.schoolsafety.gov/
	Department of Education (DoED) Readiness and Emergency Management for Schools (REMS) (教育部 (DoED) 学校准备和应急管理 (REMS)) https://rems.ed.gov/AboutUs.aspx
	SchoolSafety.gov Safety Readiness Tool (安全准备工具) https://www.schoolsafety.gov/safety-readiness-tool#no-back
	REMS Developing Emergency Operations Plans (EOPS) K-12 101 (REMS 制订应急操作计划 (EOPS) K-12 101) https://rems.ed.gov/trainings/CourseK12EOP.aspx
	REMS Guide for Developing High-Quality School Emergency Operations Plans (REMS 高质量学校应急操作计划制订指南) https://rems.ed.gov/docs/REMS_K-12_Guide_508.pdf
物理安全	CISA PSAs https://www.cisa.gov/protective-security-advisors central@cisa.dhs.gov
	DHS School Security Survey (DHS 学校安全调查) https://doe.sd.gov/schoolsafety/documents/Security-Survey-508.pdf
	REMS Live Training and Site Assess App (REMS 实时培训和场地评估应用程序) https://rems.ed.gov/SITEASSESS.aspx?AspxAutoDetectCookieSupport=1
	Partner Alliance for Safer Schools (PASS): Safety and Security Guidelines for K-12 Schools (安全学校合作伙伴联盟 (PASS): K-12 学校安保指南) https://passk12.org/wp-content/uploads/2019/01/PASS-K-12-School-Safety-Security-Guidelines-v4.pdf
	DoED Guiding Principles: A Resource Guide for Improving School Climate and Discipline (DoED 指导原则: 改善学校氛围和纪律指南) https://www2.ed.gov/policy/gen/guid/school-discipline/guiding-principles.pdf
学校氛围	School Climate Action Guide (为学校氛围行动指南) https://safesupportivelearning.ed.gov/scirp/action-guides
	USSS Analysis of Targeted School Violence (USSS 针对学校的暴力事件分析) https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.pdf
	HHS StopBullying.gov https://www.stopbullying.gov/resources/facts#stats
	USSS Enhancing School Safety Threat Assessment Model (USSS 加强学校安全威胁评估模型) https://www.cisa.gov/sites/default/files/publications/18_0711_USSS_NTAC-Enhancing-School-Safety-Guide.pdf
	University of Maryland School Health Assessment and Performance Evaluation (SHAPE) School Mental Health Profile (University of Maryland 学校健康评估和表现评估 (SHAPE) 学校心理健康档案) https://www.theshapesystem.com/wp-content/uploads/2019/10/SMH_School-version-10.2.pdf
培训	HHS Bullying Prevention Assessment Package (HHS 欺凌预防评估包) https://mchb.hrsa.gov/
	REMS Live Trainings Request (REMS 现场培训请求) https://rems.ed.gov/TA_TrainingsByRequest.aspx
	DHS Homeland Security Exercise and Evaluation Program (DHS 国土安全演习和评估计划指南) https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

资助资源

DOJ School Violence Prevention Program (DOJ 学校暴力预防方案)
<https://cops.usdoj.gov/svpp>

DOJ STOP School Violence Technology and Threat Assessment Solutions for Safer Schools Program (DOJ 安全学校方案所用的停止学校暴力技术和威胁评估解决方案)
<https://bja.ojp.gov/program/stop-school-violence-program/archives>

DoED Project School Emergency Response to Violence (SERV) Violence Recovery Support (DoED 项目学校暴力应急响应 (SERV) 暴力恢复支持)
<https://www2.ed.gov/programs/dvppserv/index.html>

DoED E-Rate Program: Cost Effective Technology to Bolster Network Infrastructure (DoED E 级方案: 具有成本效益的网络基础设施改进技术)
<https://www2.ed.gov/about/inits/ed/non-public-education/other-federal-programs/fcc.html>

第 7 章: 网络安全

网络清洁环境

CISA Cybersecurity Resources Roadmap (CISA 网络安全资源路线图)
<https://us-cert.cisa.gov/resources/smb>

CISA Cyber Essentials (CISA 网络要素)
<https://www.cisa.gov/publication/cisa-cyber-essentials>

CISA National Cyber Awareness System (NCAS): Website Security (CISA 国家网络认知系统 (NCAS): 网站安全)
<https://www.us-cert.gov/ncas/tips/ST18-006>

CISA NCAS Using Caution with Email Attachments (CISA NCAS 小心处理电子邮件附件)
<https://www.us-cert.gov/ncas/tips/ST04-010>

CISA Privacy and Mobile Device Apps (CISA 隐私和移动设备应用程序)
<https://us-cert.cisa.gov/ncas/tips/st19-003>

CISA Online Privacy Tip Sheet (CISA 在线隐私提示表)
<https://www.cisa.gov/publication/stop-think-connect-toolkit>

CISA NCAS: Staying Safe on Social Networking Sites (CISA NCAS: 在社交网站上保持安全)
<https://www.us-cert.gov/ncas/tips/ST06-003>

CISA Social Media Cybersecurity Tip Sheet (CISA 社交媒体网络安全提示表)
<https://www.cisa.gov/publication/stop-think-connect-toolkit>

CISA NCAS: Guidelines for Publishing Information Online (CISA NCAS: 在线发布信息指南)
<https://www.us-cert.gov/ncas/tips/ST05-013>

在线安全

National Cybersecurity Alliance Social Media Cybersecurity Best Practices (国家网络安全联盟社交媒体网络安全最佳实践)
<https://staysafeonline.org/resource/social-media-cybersecurity-best-practices/>

CISA NCAS: Dealing with Cyberbullies (CISA NCAS: 处理网络欺凌)
<https://www.us-cert.gov/ncas/tips/ST06-005>

CISA NCAS: Avoiding Social Engineering and Phishing Attacks (CISA NCAS: 避免社交工程和网络钓鱼攻击)
<https://www.us-cert.gov/ncas/tips/ST04-014>

CISA How to Recognize and Prevent Cybercrime Tip Card (CISA 如何识别和防止网络犯罪提示卡)
<https://www.cisa.gov/publication/stop-think-connect-toolkit>

CISA Report Cyber Incidents (CISA 报告网络事件)
<https://www.cisa.gov/reporting-cyber-incidents>
<https://us-cert.cisa.gov/report>

安全实践和认知

CISA Sign-up for US-CERT Monthly Bulletin (CISA US-CERT 月度公告打卡)
<https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new>

CISA Cyber Resilience Review (网络防范审核) (CRR)
<https://www.us-cert.gov/resources/assessments>

CISA CYBERSECURITY ADVISORS (网络安全顾问) (CSA)
<https://www.cisa.gov/csa>

	CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems (CISA 洞察见解:修复互联网可访问系统的漏洞) https://www.cisa.gov/insights
安全实践和认知 (续)	CISA Cyber Tabletop Exercise Package (网络桌面演习包) (CTEP) https://www.cisa.gov/national-cyber-exercise-and-planning-program
	DHS Handbook for Safeguarding Personally Identifiable Information (DHS 个人身份识别信息防卫讲义) https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information
恶意软件和病毒	CISA Malware Tip Card (CISA 恶意软件提示卡) https://www.cisa.gov/publication/stop-think-connect-toolkit
网络钓鱼攻击	CISA Phishing Tip Card (CISA 网络钓鱼提示卡) https://www.cisa.gov/publication/stop-think-connect-toolkit
勒索软件	CISA US-CERT Ransomware Resources (CISA US-CERT 勒索软件资源) https://www.us-cert.gov/Ransomware
	CISA NCAS: Protecting Against Ransomware Security Tips (CISA NCAS: 防备勒索软件安全提示) https://www.us-cert.gov/ncas/tips/ST19-001
网站篡改	CISA Cyber Insights: Mitigate DNS Infrastructure Tampering (CISA 网络洞察见解:缓解 DNS 基础架构篡改) https://www.cisa.gov/insights
	CISA Cyber Insights: Remediate Vulnerabilities for Internet-Accessible Systems (CISA 洞察见解:修复互联网可访问系统的漏洞) https://www.cisa.gov/insights



附录 2: 事件列表

2009

日期	HoW 名称	教派	城市, 州
2009 年 4 月 7 日	Kkottongnae Retreat Camp	基督教	Temecula, CA

John Suchan Chong, 是一名天主教静修所 69 岁的杂工, 用手枪袭击了其他居民, 这显然是对感觉自己受到轻视的报复。他开枪打死一名受害者, 打伤三人, 随后被目击者制服。

2010

2010 年 3 月 20 日	Church of the Living God	基督教	Pittsburg, CA
--------------------	--------------------------	-----	---------------

42 岁的 John Hugo Scherzberg 对自己的生活境况极为不满, 并将其归咎于上帝, 纵火焚烧了数座教堂。

2011

2011 年 6 月 1 日	St. Ambrose Cathedral	基督教	Des Moines, IA
-------------------	-----------------------	-----	----------------

通过一次秘密的网络攻击, 黑客窃取了教区为帮助无家可归者和受虐妇女而筹集的 68 万多美元。

2012

2012 年 1 月 1 日	Imam Al-Khoel Foundation	伊斯兰教	New York City, NY
-------------------	--------------------------	------	-------------------

40 岁的 Ray Lazier Legend 也被人称为 Suraj Poonai, 他用燃烧弹烧毁了数座住宅和宗教场所, 包括一座印度教寺庙和一座清真寺, 宣称他想“消灭尽可能多的阿拉伯人”。没有人受伤, 但袭击导致重大财产损失。

2012 年 1 月 12 日	Congregation Beth El	犹太教	Paramus, NJ
--------------------	----------------------	-----	-------------

Anthony Graziano 和 Aakash Dalal 在犯罪时分别为 19 岁和 20 岁, 一开始是反犹太主义, 后来发展为用燃烧弹袭击了两座犹太教堂和一名拉比家。

2012 年 5 月 12 日	St. Peter's Episcopal Church	基督教	Ellicott City, MD
--------------------	------------------------------	-----	-------------------

56 岁的 Douglas Franklin Jones 在一场有关 教堂食品储藏室的争执中枪杀了一名圣公会牧师和教堂秘书。

日期	HoW 名称	教派	城市, 州
2012 年 5 月 20 日	New Holy Deliverance Outreach Ministry	基督教	Axton, VA
17 岁的 Jean-Claude Bridges 和一名未透露姓名的青少年同谋烧毁了一座以黑人为主的教堂。在审判中, 他承认是出于种族偏见选择教堂作为目标。			
2012 年 8 月 5 日	Oak Creek 的 Sikh Temple of Wisconsin	锡克教	Oak Creek, WI
40 岁的退伍军人 Wade Michael Page 与白人至上主义组织有联系, 他在一座锡克教寺庙开枪打死了 6 人。另有四人在袭击中受重伤, 其中包括一名警官; 一名牧师后来因伤势过重死亡。枪手被警官射伤, 随后自杀。			
2012 年 8 月 6 日	Islamic Society of Joplin	伊斯兰教	Joplin, MO
32 岁的 Jedediah Stout 在纵火焚烧一家计划生育诊所后被捕。在审判中, 他承认了几项纵火指控, 并承认因为不喜欢伊斯兰教而烧毁了一座清真寺。			
2012 年 9 月 30 日	Islamic Center of Greater Toledo	伊斯兰教	Perrysburg, OH
52 岁的卡车司机、前海军陆战队队员 Randolph T.Linn 在数小时后闯入一座清真寺, 纵火焚烧了祈祷室, 造成超过 100 万美元的损失。在审判中, Linn 承认他一直酗酒, 并对中东发生的针对美国军人袭击事件的震撼新闻报道感到不安。			
2012 年 10 月 1 日	Temple Kol Ami Emanu-El	犹太教	Plantation, FL
一群自称 Team System Dz 的黑客在一个宗教节日期间入侵了一个犹太教堂网站, 将网站内容换成反犹太主义信息和对伊斯兰国恐怖组织的赞扬。			
2012 年 10 月 24 日	World Changers Church International	基督教	College Park, GA
51 岁的 Floyd Palmer 枪杀了一名在 Atlanta 地区一座大教堂主持祈祷仪式的教堂志愿者。Palmer 的动机尚不清楚, 但他之前曾因 Baltimore 清真寺枪击案被指控, 并有精神病史。			
2012 年 12 月 2 日	First United Presbyterian Church	基督教	Coudersport, PA
Gregory Eldred 是一名 52 岁的学校教师, 在一次教堂礼拜中找到了他的前妻, 并在她弹风琴时开枪打死了她。Eldred 被判处死刑, 他的动机仍在调查中。			

2013

日期	HoW 名称	教派	城市, 州
2013 年 3 月 31 日	Hiawatha Church of God in Christ	基督教	Ashatabula, OH

28岁的 Reshad Riddle 在复活节教堂的一次礼拜中枪杀了他的父亲,并在持枪指向他人时发表了杂乱无章的言论。Riddle 很快被警官制服。法官认定 Riddle 属于法律上界定的精神错乱,并将其送至行为医疗系统拘押。

2013 年 10 月 8 日	Spring Valley Catholic Church	基督教	Spring Valley, CA
--------------------	-------------------------------	-----	-------------------

46岁的 Eugene William Volk 承认了一系列指控,包括与教堂起火有关的仇恨犯罪和纵火,这场火灾造成了超过 20 万美元的损失。Volk 有很多犯罪记录,并承认憎恨天主教信仰。

2014

2014 年 4 月 13 日	Jewish Community Center of Greater Kansas City	犹太教	Overland Park, KS
--------------------	---	-----	-------------------

73 岁的退伍军人 Frazier Glen Miller, Jr. 长久以来一直与种族主义组织有联系,他在一个犹太社区中心和退休社区开枪打死了三人。

2015

2015 年 6 月 17 日	Emanuel African Methodist Episcopal Church	基督教	Charleston, SC
--------------------	---	-----	----------------

21 岁的白人至上主义者 Dylan Roof 在一座历史悠久的黑人教堂的祈祷仪式上开枪打死 9 人。Roof 在被捕期间表示,他的意图是发动一场种族战争。

2015 年 9 月 13 日	Corinth Missionary Baptist Church	基督教	Bullard, TX
--------------------	-----------------------------------	-----	-------------

40 岁的 Rasheed Abdul Aziz 身穿全套战术装备,手持手枪进入一座教堂,宣称他打算“杀死异教徒”,这位牧师是一位经验丰富的危机干预专家,他说服了此人,阻止了枪击案的发生。枪手于第二天被捕。

2015 年 12 月 11 日	Islamic Society of Coachella Valley	伊斯兰教	Coachella, CA
---------------------	-------------------------------------	------	---------------

刚过中午,23 岁的 Carl James Dial 向一座清真寺投掷了一个燃烧瓶。没有人受伤,但大火导致重大财产损失。Dial 的父母称他情绪混乱,调查人员认为这次袭击是对 2015 年 San Bernadino 大规模枪击事件的报复。

2016

2016 年 1 月 1 日	Islamic Center of Wheaton	伊斯兰教	Chicago, IL
-------------------	---------------------------	------	-------------

不知名的黑客为 Chicago 地区的一座清真寺创建了一个虚假网站,并发布了煽动性的图片和信息,引发了反穆斯林的反弹。

日期	HoW 名称	教派	城市, 州
2016 年 2 月 28 日	St. Peter's Missionary Baptist Church	基督教	Dayton, OH
68 岁的 Daniel Schooler 在一场诉讼纠纷中枪杀了他的牧师兄弟。在审判中, Schooler 解释说, 他去教堂讨论这场争执, 并在争论激烈后出于自卫向他的兄弟开枪。Schooler 有很长的犯罪记录和精神病史。			
2016 年 8 月 13 日	Al-Furqan Jame Masjid Mosque	伊斯兰教	New York City, NY
35 岁的 Oscar Morel 在两名穆斯林学者离开纽约一座清真寺时开枪打死了他们。法官判处 Morel 终身监禁, 但调查人员无法确定其动机。			
2016 年 9 月 1 日	Hopewell Missionary Baptist Church	基督教	Greenville, MS
47 岁的 Andrew McClinton 烧毁了 Mississippi 州一座历史悠久的黑人教堂。McClinton 有很多犯罪记录, 调查人员认定他烧毁自己所在的教堂是为掩盖非法活动。			
2016 年 9 月 11 日	Islamic Center of Fort Pierce	伊斯兰教	Fort Pierce, FL
32 岁的 Joseph Schreiber 纵火焚烧了 Omar Mateen 以前去过的一座清真寺, 后者在 Orlando 的 Pulse 夜总会实施了大规模枪击清真寺被损毁。Schreiber 此前曾在社交媒体上发布反伊斯兰信息, 并在审判中发表仇视伊斯兰教的言论。			
2017 年 1 月 7 日	St. Stephen Presbyterian Church	基督教	Fort Worth, TX
54 岁的 Thomas Dale Britton 连夜闯入一座教堂, 花了数小时破坏教堂并纵火, 造成 50 多万美元的损失。他留下了意指 ISIS 的图画和文字, 但调查人员无法确定其动机。			
2017 年 2 月 17 日	St. Augustin Church	基督教	Des Moines, IA
31 岁的 Ashley Eckhardt 在一名天主教执事为病人服务时进行了持刀袭击。目击者称 Eckhardt 精神紊乱, “大叫魔鬼”。执事幸免于难; 法官判处 Eckhardt 五年有期徒刑。			
2017 年 6 月 11 日	Islamic Society of Tampa	伊斯兰教	Pomona, CA
42 岁的退伍军人 Shaun Urwiler 患有创伤后应激障碍, 他的卡车撞上了几辆汽车, 然后撞穿了一座清真寺的大门, 造成约 6000 美元的损失。在被捕时, Urwiler 告诉警官, 他想“制造一点破坏”。			

2017

日期	HoW 名称	教派	城市, 州
2017 年 8 月 5 日	Dar al-Farooq (DAF) Islamic Center	伊斯兰教	Bloomington, MN

三名男子 - 29 岁的 Michael McWhorter; 23 岁的 Joe Morris 和 47 岁的 Michael Hari 试图在晨祷时向一座清真寺扔炸弹。McWhorter 和 Morris 承认多项仇恨犯罪指控; Hari 正在等待审判。三人都与白人至上组织有联系。这次爆炸是多州犯罪狂潮的一部分, 目的是将穆斯林驱逐出境。

2017 年 9 月 24 日	Burnette Chapel Church of Christ	基督教	Antioch, TN
--------------------	----------------------------------	-----	-------------

25 岁的 Emanuel Kidega Samson 在 Burnette Chapel Church of Christ (位于 Tennessee 州 Antioch 市) 的停车场开枪打死一人。Samson 进入教堂继续进行袭击。在执法部门逮捕 Samson 之前, 他总共杀死了一人, 打伤了七人。

2017 年 11 月 5 日	First Baptist Church	基督教	Sutherland Springs, TX
--------------------	----------------------	-----	------------------------

26 岁的 Devin Patrick Kelley 在 Texas 州 Sutherland Springs 的 First Baptist Church 开枪打死 26 人, 打伤 20 人。他一开始在停车场开枪射击, 然后进入教堂继续袭击。教堂一名持合法枪支的邻居向 Bowers 开了两枪, 并开车追赶袭击者。Bowers 的车撞翻了, 在警察到来之前, 他用手枪自杀了。

2018

2018 年 10 月 27 日	Tree of Life Synagogue	犹太教	Pittsburgh, PA
---------------------	------------------------	-----	----------------

46 岁的 Robert Gregory Bowers 在 Pennsylvania 州 Pittsburgh 的 Tree of Life Congregation 开枪打死 11 人, 打伤 6 人, 其中包括 4 名执法人员。在逮捕袭击者前, 警方与其交火。Bowers 面临多项联邦和州指控, 包括仇恨犯罪。

2018 年 11 月 23 日	Congregation Bais Yeshuda	犹太教	Los Angeles, CA
---------------------	---------------------------	-----	-----------------

32 岁的 Mohamed Mohamed Abdi 试图用车碾压离开 California 州 Los Angeles 的 Congregation Bais Yeshuda 的礼拜者。没有伤亡报告。当局追踪并逮捕了袭击者, 他在袭击中大喊反犹太主义。

2019

2019 年 4 月 1 日	St. Ambrose Catholic Church	基督教	Brunswick, OH
-------------------	-----------------------------	-----	---------------

Ohio 州 Brunswick 的 St. Ambrose Catholic Church 在一次网络攻击中损失了 175 万美元的翻修资金。犯罪者冒充建筑公司侵入教堂的电子邮件。他们利用电子邮件向另一名员工索取财务信息。

日期	HoW 名称	教派	城市, 州
2019 年 4 月 4 日	St. Mary Baptist Church/Greater Union Baptist Church/Mount Pleasant Baptist Church	基督教	Port Barre; Opelousas, LA
<p>21 岁的 Holden Matthews 在几个晚上烧毁了 Louisiana 州的四座教堂。他袭击了 Louisiana 州的 St. Mary Baptist Church (Port Barre)、Greater Union Baptist Church 和 Mount Pleasant Baptist Church (Opelousas) Matthews 在互联网上分享了有关袭击的视频和图像。Matthews 面临数项州犯罪指控。</p>			
2019 年 4 月 27 日	Chabad of Poway Synagogue	犹太教	Poway, CA
<p>19 岁的 John Timothy Earnest 在 Chabad of Poway Synagogue 发生的枪击案中造成一人死亡, 三人受伤。San Diego Police Department 在距犹太教堂约两英里的地方逮捕了 Earnest。袭击发生在逾越节的最后一天。</p>			
2019 年 12 月 29 日	West Freeway Church of Christ	基督教	White Settlement, TX
<p>43 岁的 Keith Kinnunen 在 Texas 州 White Settlement 一座教堂周日上午的礼拜中开枪打死两人。他乔装打扮实施了这次袭击。教堂的保安队长开枪打死了 Kinnunen。</p>			
2019 年 12 月 29 日	Congregation Netzach Yisroel	犹太教	Monsey, NY
<p>37 岁的 Grafton Thomas 被控在 New York 的 Monsey 由一名拉比举办的光明节庆祝活动上用利器袭击数人。他被宣布不适合接受审判, 目前在精神病院接受治疗。</p>			





U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

Washington, D.C. 20528