

Principal Brief // two-minute read

- MONITORING & ALERTING
- THREAT DOCTRINE
- EXECUTIVE PROTECTION

Someone Usually Notices First



Removing your data lowers what an adversary can find. It does not tell you who is already looking. In the studies, most attackers showed warning signs first, and many of those signs reached people around them before anything reached a place a search could find.

WHAT THE RECORD SHOWS

People who attacked prominent figures never threatened their targets first, but three-quarters talked or wrote about the target to someone else. Three-quarters of mass attackers worried someone beforehand; about a quarter said something concerning online. When a warning sign was reported, most plots were stopped.

WHY IT REACHES YOU

Monitoring that only searches the internet, or waits for a threat addressed to you, watches one part of the picture. The rest reaches you only if someone who notices has a way to tell you, and a reason to think you will act.

THREE THINGS TO TAKE FROM THIS

- 1

Removal is not monitoring

Checking that your records stay deleted watches your data. Monitoring watches who is paying attention.
- 2

Don't wait for a threat

Fixation, preparation and approach often come without a threat ever sent to you.
- 3

Search, and be reachable

Watch what is public, and give the people who see the rest a clear way to report it.

DO THIS

- ☐

YOU, WITH YOUR MONITORING PROVIDER

Ask what they escalated last quarter, what happened next, and what they cannot see.
- ☐

YOU, WITH YOUR FAMILY OFFICE

Set up one clear channel for staff, family and contacts to report a worrying contact.
- ☐

YOU, WITH YOUR SECURITY LEAD

Agree in advance who assesses reports, who can act, and when police are called.

NOT THE STORY YOU MAY HAVE HEARD

Monitoring is not a keyword alert that catches every threat, and silence is not safety. Most hostile talk is venting, and the plans that matter are often private until shortly before. Its value is time and triage, not omniscience.

HOW SURE WE ARE

High on the research findings and the case record. High that a public search sees only part of the warning signs; how large a part is not measured. Not established: how often a two-channel program prevents an attack.

THE FULL COMMAND BRIEF FOLLOWS: THE RECORD, WHERE WARNING SIGNS APPEAR, TRIAGE, AND POSTURE.

CB-084

Active threat monitoring: search what you can, hear what you can't



"Removal lowers what an adversary can find. Monitoring shows who is already looking, when they show it."

The v1 of this brief argued, from practice, that hostile intent usually becomes visible before it becomes action. The research supports the timing and widens the location: warning signs reach people around an attacker, often well before anything reaches a place a search could find, and attackers of prominent figures rarely threaten their targets first.

BLUF. Re-checking whether removed records reappear watches the principal's data and belongs to the removal program (CB-107). Active threat monitoring watches who is paying attention: anyone discussing, doxxing, coordinating against or moving toward the principal. The governing frame is time; intent caught early is a referral or a change of plans, and caught late it is an incident. The record supports the premise and widens where to look. The Secret Service's study of the 83 people who attacked or came close to attacking prominent figures from 1949 to 1996 found no attacker communicated a direct threat to the target or to police beforehand, while 77 percent communicated about the target to someone, usually not the target. Its 2023 study of 173 mass attacks found three-quarters of attackers showed concerning behavior and communications, mostly noticed by family, friends, neighbors and coworkers; nearly a quarter conveyed concerning communications online. The FBI found 56 percent of 63 active shooters leaked intent, and no bystander reported that leakage to police. RAND found that plots were foiled more than 80 percent of the time when an initial warning sign was reported, and less than 5 percent when none was. Monitoring therefore needs two channels, a search of what can be found and a way to hear from people who see what cannot, feeding one assessment against criteria agreed in advance. Neither is complete, and whether the pair prevents harm depends on what happens next.

0 Attackers of prominent figures who sent a direct threat to the target or police first. SECRET SERVICE, 1999	3 in 4 Mass attackers who showed concerning behavior and communications; about 1 in 4 online. SECRET SERVICE, 2023	56% Active shooters who leaked intent; no bystander reported the leakage to police. FBI, JUNE 2018	>80% Plots foiled when a warning sign was reported, against under 5% when none was. RAND, 2022
--	---	---	--

Removing the data does not tell you who is hunting it.

SECRET SERVICE, ATTACKS ON PROMINENT FIGURES, 1999

The Exceptional Case Study Project examined all 83 people known to have attacked or approached to attack a prominent person in the United States from 1949 to 1996, in 34 attacks and 40 near-lethal approaches; targets included officials, celebrities and corporate executives. No assassin or attacker communicated a direct threat to the target or to police beforehand, and fewer than a tenth of all 83 did. Yet 77 percent communicated about the target: to family (22 percent), friends (18 percent), others (47 percent) or in diaries. One explained why he sent no letter: "the police would have come and arrested me. I didn't want to be stopped then." For a principal, this is the closest study in the record: the warning arrives sideways, not addressed to the target.

SECRET SERVICE, MASS ATTACKS, JANUARY 2023

The National Threat Assessment Center reviewed 173 attacks by 180 attackers in public places from 2016 to 2020. Three-quarters exhibited concerning behaviors and communications, and most had elicited concern in family members, friends, neighbors, coworkers, school staff or officials. Nearly a quarter conveyed concerning communications online. Many made threats, often without specifics.

FBI, JUNE 2018

The Behavioral Analysis Unit's study of 63 active shooters found 56 percent leaked intent to commit violence (51 percent of adults, 88 percent of those under 18). Concerning behavior was noticed mostly through what shooters said (95 percent) and did (86 percent); it showed online in 16 percent. Observers most often spoke to the shooter or did nothing; concerning behavior reached police in 41 percent of cases, but "no bystanders reported instances of leakage to law enforcement." In 65 percent of cases no threat was made to a target, and the FBI warns that the absence of a direct threat "should not be falsely reassuring."

AVERTED PLOTS, SECRET SERVICE 2021, AND RAND 2022

Of 67 averted school attack plots from 2006 to 2018, about 94 percent of plotters had communicated their intentions in some way, and about three-quarters of plots were detected because of those communications. RAND's study of mass attacks and plots from 1995 to 2020 found about two-thirds of prevented plots were foiled through reporting by the public.

PRIVATE CHANNELS, BUFFALO, MAY 2022

The Tops Friendly Market shooter kept a private Discord diary of his plans for months. Discord said a small group was invited to see it about 30 minutes before the attack. It was invisible to an outside search, and to most people near him, until the end.

FROM REPORT TO ACTION, 2025 AND 2026

Capitol Police opened 14,938 threat assessment cases on members of Congress in 2025, up from 9,474. In one, its Threat Assessment Section issued a lookout bulletin on 28 October and officers stopped the subject at the Russell Senate Office Building on 4 November, before screening. In the alleged UFC plot (CB-082), a parent's call started the investigation and messages on one phone identified the rest: human observation first, digital evidence second.

FIGURE 1 // WHERE WARNING SIGNS APPEAR, AND WHAT CAN SEE THEM

WHERE	ON THE RECORD	VISIBLE TO A SEARCH?	CONTROL
PUBLIC POSTS AND FORUMS	About a quarter of mass attackers; 16% of active shooters	Partly; online is not always searchable	Analyst-reviewed search of open and fringe sources
CONTACT WITH THE PRINCIPAL	Capitol Police: mail, email, phone, social	Yes, through the principal's own inbound	Route inbound to one triage point
EXPOSURE OF THE PRINCIPAL	Doxxing, circulating addresses (CB-061, CB-083)	Yes	Watch for the principal's details, not only threats
PEOPLE NEAR THE SUBJECT	Most assassins told someone; FBI: leakage not reported	No, unless they report	Tip lines, police and partner relationships
PEOPLE NEAR THE PRINCIPAL	Approaches, odd contacts, probing	No, unless they report	A known channel for staff and family, and follow-up
PRIVATE CHANNELS	Buffalo diary, seen 30 minutes out	No, until shared	Nothing from outside

THE MECHANISM // WHY TIME, AND WHY TWO CHANNELS

M1 INWARD CONTROLS ARE SILENT ON ATTENTION

Removal and disclosure discipline (CB-107, CB-083) reduce what a principal exposes. They say nothing about who is paying attention or why. A principal can hold a minimized footprint and still be the subject of a doxxing thread, a target list, a harassment campaign (CB-062) or a fixated individual.

M2 THE THREAT THAT NEVER THREATENED YOU

Attackers of prominent figures did not threaten their targets first; the study's authors concluded that attention belongs on behavior suggesting a threat, whether or not a threat is ever sent. Monitoring that keys on threats addressed to the principal watches the wrong signal. Fixation, research on the principal's movements, preparation and approach can matter more than threatening language, and they show up across different people and places.

M3 SEEN BEFORE SEARCHABLE

Three-quarters of mass attackers concerned someone; about a quarter said something concerning online. Among active shooters, concerning behavior showed online in 16 percent of cases, against 95 percent through speech. The groups overlap, and online is not the same as searchable, so the studies do not measure how much a commercial search can see. They do show that a search watches one subset of the warning signs, and that the rest reaches a protective team only if someone reports it.

M4 ONE ASSESSMENT, AND SOMEONE WHO CAN ACT

Hostile talk about a public figure is large, mostly inert and often unspecific; keyword alerts drown a team. Signals from both channels need correlating, validating and prioritizing in one process, against criteria weighed in combination rather than as a ladder, and someone with the authority to act on the result.

► THE TEST

Ask whoever monitors for the principal: what did you escalate last quarter, what can you not see, and if a driver or a neighbor saw something worrying tomorrow, how would it reach you? *If the third answer is "they would call someone they know," the second channel is unmanaged.*

FIGURE 2 // TRIAGE SIGNALS, WEIGHED IN COMBINATION, NOT IN SEQUENCE

VENTING	Hostile but general, no target detail or plan. Log it; look for repetition by the same source.
FIXATION	Repeated, personal focus on the principal or family. Watch; assess with a threat professional.
EXPOSURE	Address, schedule or family details circulating. Change posture; remove or contain.
PREPARATION, APPROACH	Research on movements, acquiring means, showing up or probing. Escalate, whatever the language.
COORDINATION	Target lists, calls to act, groups organizing. Escalate; consider a referral to police.
IMMINENCE	Signs that action is near. Contact law enforcement now; specifics are not required.

FIGURE 3 // PROPOSED ARCHITECTURE: TWO CHANNELS, ONE ASSESSMENT

CHANNEL 1: DIGITAL DISCOVERY	Public posts and forums, doxxing and coordination, exposure of the principal, inbound contact, fixation and narrative signals.
CHANNEL 2: HUMAN REPORTING	Staff and family, third-party observers, direct contacts, and referrals from police and security partners, who reach the subject's circle as a principal's staff cannot.
UNIFIED ASSESSMENT	Correlate, validate and prioritize signals from both channels, with context and corroboration.
MANAGEMENT	Someone with authority acts: referral, posture change, intervention, and follow-up over time.

DOCTRINE, NOT DATA

A proposed design consistent with the studies, not drawn from them. Neither channel alone is complete.

THE STEELMAN // THE CASE THAT MONITORING IS NOISE

THE STRONGEST VERSION OF THE OPPOSING VIEW

- + The hostile conversation is enormous and mostly venting; Capitol Police volume shows the scale.
- + Most threats never become action, and real plans stay private.
- + A reporting channel invites false and malicious reports, mistaken attribution, privacy costs and expensive chases.

Concede all three; they are real costs. That is why both channels feed one analyst-led assessment rather than a keyword alert or a hotline that triggers action on its own, and why reports are corroborated before anyone acts on them (CB-061 covers the malicious kind). The value is not catching every angry post. It is surfacing fixation, preparation, exposure and coordination while intent is still a referral, and hearing from people who see what no search can. The record on averted plots shows that path works when a report is made.

ASSESSMENT

Attackers in the studied populations usually showed warning signs first.	STRONG / SECRET SERVICE, FBI
Attackers of prominent figures did not send direct threats to targets or police.	STRONG / SECRET SERVICE 1999

Many signs are seen by people nearby; a public search sees only a subset.	STRONG / STUDIES
Reported warning signs are associated with plots being foiled.	STRONG / RAND, AVERTED PLOTS
The share of warning signs visible to commercial monitoring.	NOT MEASURED
A two-channel private program measurably reduces attacks.	NOT ESTABLISHED

POSTURE

FOR PRINCIPALS

- Treat who is paying attention as a standing question; pair removal with monitoring.

FOR FAMILY OFFICES

- Commission analyst-reviewed monitoring, separate from regrowth checks, and ask what it cannot see.
- Give staff, family and close contacts one known channel to report a worrying contact, and close the loop.

FOR SECURITY AND LEGAL FUNCTIONS

- Run both channels into one assessment (Figure 3), and name who can act on it.
- Escalate on preparation and approach, not only on threats; build police and partner relationships before you need them.

CONFIDENCE High on the research findings and the case record. High that a public search sees only part of the warning signs; the size of that part is not measured. Not established: whether a two-channel private program reduces attacks.

METHOD Revised edition. First published 1 June 2026; facts gathered and analysis revised 14 October 2026. The v1 doctrine is kept, its timing claim calibrated against the studies. Following external review, the FBI figures are checked against the full report and corrected to 56 percent overall, the attacks-on-prominent-figures, averted-plot and RAND findings are added, and triage is weighed in combination.

SOURCES Fein and Vossekuil, [Assassination in the United States](#), Journal of Forensic Sciences, March 1999; [Secret Service NTAC, Mass Attacks in Public Spaces: 2016 to 2020](#), January 2023; Silver, Simons and Craun, [A Study of the Pre-Attack Behaviors of Active Shooters](#), FBI, June 2018; Secret Service NTAC, [Averting Targeted School Violence](#), March 2021, figures via [AP](#); [RAND, Mass Attacks Defense Toolkit](#), 2022; [AP, 18 May 2022](#); U.S. Capitol Police, [27 January 2026](#) and [4 November 2025](#); CB-082.

Scope note: most studies cover mass attacks and shooters; the 1999 study covers attacks on prominent figures. This is intelligence analysis, not legal advice.