APCO International
Leaders in Public Safety Communications®

PSTA
Public Safety Threat Alliance
Public Safety ISAO

Public Safety Threat Report:
Swatting in emergency communications

Disclosure protocol: GREEN: Restricted to the community
Date of writing: 05 June 2026

Executive Summary

Swatting has emerged as a high impact threat that directly challenges emergency communications centers (ECCs) and other fellow first responders. Recent incidents reported nationally illustrate the scale and seriousness of this threat. In early 2026, multiple university campuses were evacuated following coordinated hoax threats that triggered significant law enforcement responses.[1] Similar swatting events targeted public venues such as zoos and government facilities, resulting in lockdowns, evacuations and widespread service disruptions.[2] These incidents demonstrate how cyber threat actors use digital tools to manipulate emergency response systems, creating immediate physical risk to public safety telecommunicators (PSTs), field responders and the public. As swatting tactics continue to evolve, ECCs are increasingly required to operate at the intersection of cyber deception and real-world emergency response.

Findings from the 2026 APCO and PSTA ECC Swatting Survey reinforce the growing operational strain swatting places on public safety agencies. The majority of responding ECCs reported experiencing at least one swatting incident within the previous year, with many managing repeated events. Survey results identified a significant gap in preparedness, including limited availability of swatting specific training, inconsistent PST confidence levels and the absence of written standard operating procedures (SOPs) for handling swatting incidents in many ECCs. Respondents also highlighted persistent challenges related to caller ID spoofing, Voice over Internet Protocol (VoIP) services, and emerging technologies such as synthetic or recorded audio. In addition, the survey revealed fragmented coordination and reporting practices with limited information sharing across jurisdictions and no uniform approach to tracking swatting incidents.

> *As swatting tactics continue to evolve, ECCs are increasingly required to operate at the intersection of cyber deception and real-world emergency response.*

Based on these findings, this report recommends a coordinated set of actions to strengthen public safety resilience against swatting. Priority recommendations include the development and adoption of standardized swatting specific policies and SOPs, expanded scenario-based training for PSTs and supervisors, and targeted investments in call handling and verification workflows. The report also emphasizes the need for stronger interagency coordination with law enforcement, telecommunications providers, cybersecurity partners and intelligence organizations, as well as improved tracking and reporting practices to support trend analysis and threat identification. Together, these actions support a strategic shift toward treating swatting as a cyber physical risk that requires integrated planning, sustained investment and cross sector collaboration.

1 University of Wisconsin–Parkside. (2026, February 21). UW–Parkside threat investigation, campus reopens [News article]. FOX6 News Milwaukee. https://www.fox6now.com/news/uw-parkside-campus-threat-evacuation-shelter-place-order-issued

2 Associated Press. (2026, May 3). Hoax calls spark evacuations and closures at U.S. zoos [News article]. AP News. https://www.apnews.com/article/zoo-swatting-threats-04689c0a6ea174a46132c6c686db00e4

Introduction

Swatting is a malicious tactic that exploits emergency response systems by deliberately reporting fabricated, high-risk incidents to provoke an immediate and substantial law enforcement response at a targeted location. The Federal Bureau of Investigation (FBI) defines swatting as the act of making hoax calls or reports to emergency services, typically alleging an imminent threat to life, with the intent of generating a tactical or large-scale response to unsuspecting victims.[3] These incidents are designed to create fear, disruption and potential physical harm while diverting limited public safety resources from legitimate emergencies. As documented throughout this report, swatting has evolved from isolated prank behavior into a coordinated, technology-enabled threat that exploits emergency communications infrastructure, open source personal data and the operational realities of modern emergency communications.

For ECCs, swatting represents a complex cyber physical risk that directly challenges traditional call handling and dispatch models. PSTs must operate within a no fail environment where reports of violent crime demand immediate action, even as adversaries increasingly leverage caller ID spoofing, VoIP services, synthetic audio and scripted narratives to manipulate emergency response. This convergence of technological deception and real-world consequences places public safety agencies in a position where rapid response and analytical verification must occur simultaneously, often under extreme time pressure.

Addressing this threat requires a deliberate focus on training, policy and coordination. As this report demonstrates, gaps in swatting-specific training, inconsistent confidence levels among PSTs, the absence of written SOPs and limited cross jurisdictional coordination collectively increase operational risk. Strengthening these foundational elements is essential to improving situational awareness, supporting safer response strategies and reducing the likelihood that malicious false reports escalate into dangerous or unnecessary field deployments.

Methodology

This report is informed by findings from the 2026 APCO and PSTA ECC Swatting Survey, which was distributed to and completed by APCO International members and industry contacts, who work within the public safety communications community. The survey was open from December 4, 2025, through January 30, 2026, and multiple reminder emails were sent during the collection period to encourage participation. A total of 766 unique responses were received.

The survey instrument focused on capturing both quantitative and qualitative insights related to swatting incidents experienced by ECCs. Key topic areas included the frequency and types of swatting incidents, common targets and fabricated scenarios, technologies observed during swatting events, training availability and perceived effectiveness, PST confidence levels, the presence or absence of written SOPs, and coordination and reporting practices with law enforcement and external partners. Responses were self-reported and reflect the operational perspectives and experiences of participating members during the survey timeframe.

Survey data was aggregated and analyzed using descriptive statistical methods to identify trends and patterns across responses. Open-ended responses were reviewed to identify recurring themes related

3 Federal Bureau of Investigation. (2025, April 29). Threat actors use swatting to target victims nationwide (Alert No. I 042925 PSA). https://www.fbi.gov/investigate/cyber/alerts/2025/threat-actors-use-swatting-to-target-victims-nationwide

to operational challenges, training gaps and coordination needs. The analysis was designed to provide a snapshot of current practices and emerging risks rather than to establish causal relationships or longitudinal trends. As with all voluntary surveys, findings may reflect response bias and varying interpretations of terminology across agencies.

Several scope limitations should be acknowledged when interpreting the results. The survey captures a point-in-time view of swatting activity and preparedness and does not measure changes over time. Additionally, inconsistencies in how agencies define, classify and log swatting incidents may result in underreporting or misclassification. Despite these limitations, the survey provides valuable insight into the current operational landscape and highlights critical areas where training, policy development and coordination can strengthen public safety resilience against swatting incidents.

Swatting Incident Trends

The statistical surge in swatting reveals a trend that has evolved beyond localized mischief. For ECC leadership and frontline personnel alike, the survey points to swatting as a significant operational challenge that actively turns emergency systems against innocent citizens, transforming traditional, rapid-dispatch communications floors into high-stakes threat verification and risk-triage environments.

Frequency of Swatting Incidents Reported by Agencies

The 2026 APCO and PSTA ECC Swatting Survey tells a story that PSTs already know firsthand: swatting is no longer an occasional prank. It has become a predictable, recurring drain on daily public safety operations that risks the lives of first responders and innocent citizens alike. Out of the 766 respondents in the 2026 APCO and PSTA survey, an overwhelming 641 respondents had to manage

at least one swatting incident over the last year. When you break down the volume, the pressure on ECCs becomes clear: 473 ECCs handled between 1 and 5 swatting events, 100 ECCs processed between 6 and 10, and a heavily targeted tier of 68 agencies responded to more than 10 swatting events in a single 12-month window. Only 65 agencies reported a clean slate with zero incidents. Perhaps the most telling statistic for directors is that 60 centers couldn't even track the metric, in part due to legacy logging platforms. This means our true baseline is almost certainly higher than what the survey numbers show.

Most Common Targets

> *"Swatting is no longer an occasional prank. It has become a predictable, recurring drain on daily public safety operations that risks the lives of first responders and innocent citizens alike.*

Often, threat actors aren't throwing darts at a map to select their victims. They choose their targets carefully to trigger maximum law enforcement response, dominate news cycles or inflict maximum psychological distress on a specific victim. The survey data, coupled with APCO International and PSTA intelligence analysis, identifies distinct top targets for swatting attacks: homes/general residents of the public, schools and campuses; businesses and hospitals; and public officials' homes.

Private homes are the most frequent targets, often caught in the crossfire of online gaming disputes, personal vendettas, financial extortion or malicious doxxing

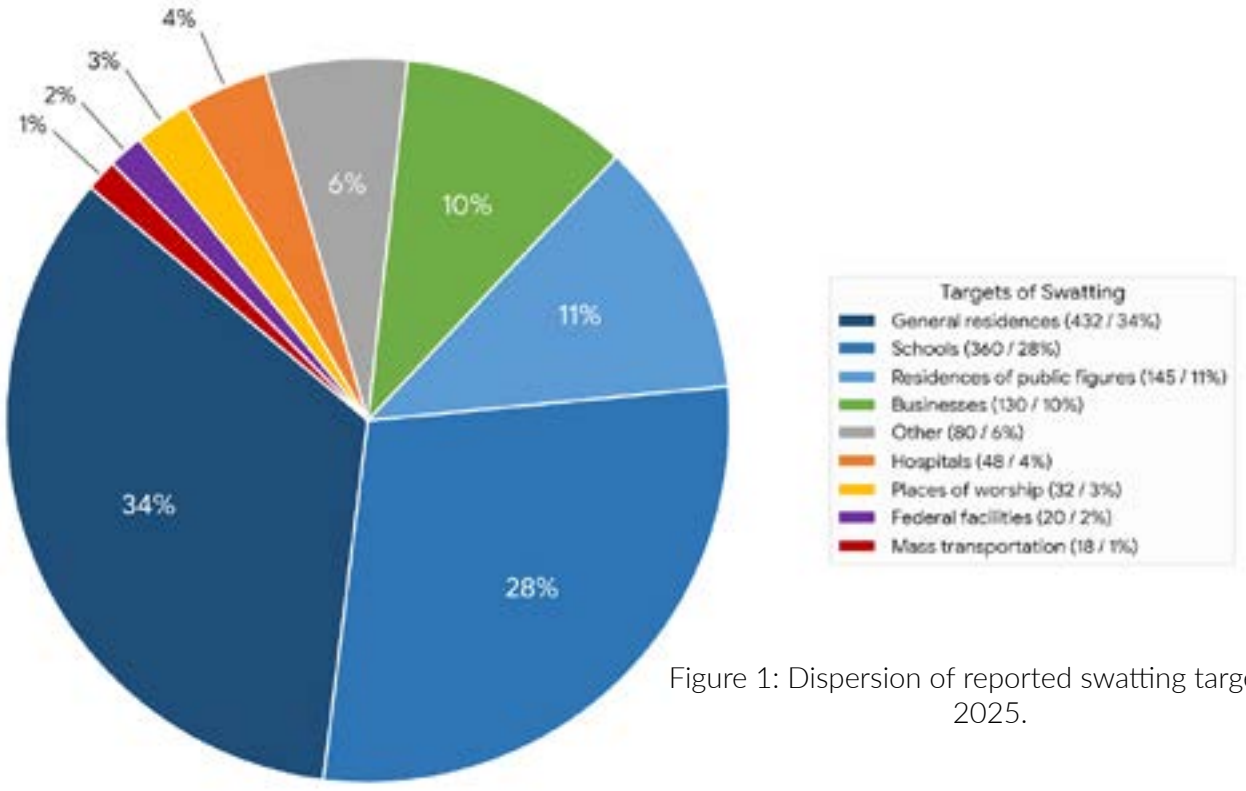

Figure 1: Dispersion of reported swatting targets in 2025.

campaigns. For a PST, these are incredibly high-risk situations because responding patrol officers arrive at a quiet home expecting a violent active crime scene. This creates an immediate risk of an accidental escalation with an innocent homeowner. In February 2026, a VOIP call was made to a law enforcement agency by someone claiming they just shot their wife.[4] Deputies found no merit to the call upon

4 Northern California Regional Intelligence Center (NCRIC). "Suspicious Activity Report 2026-0000250-SAR." Partner Update Brief. February 18, 2026.

arrival. The targeted address belonged to an online gaming company employee who had been swatted previously, and a similar call was placed to an out-of-state department from the identical phone number.

K-12 buildings and university campuses are chosen explicitly because they can spark an immediate response and corresponding panic. During the 2023-24 school year alone, there were more than 850 verified school swatting calls in the U.S.[5] In 2025 the "Purgatory" group hit 10 major universities simultaneously using Google Voice numbers.[6] In April 2026, A male caller threatened to "shoot up" a middle school with an AR-15 rifle.[7] The caller stated his motive was "because that is what we do," and threatened the family of the staff member who answered the phone. For an ECC, a school swatting event isn't just one bad call; it can lead to radio channels paralyzed by mutual aid coordination, while phone lines are overwhelmed by terrified parents.

Commercial hubs, shopping plazas, transport links and medical facilities represent an expanding target vector. A swatting event in 2026 targeted a regional airport terminal.[8] The caller claimed to have placed multiple active explosive devices. Such scenarios can freeze commercial operations, force time consuming tactical searches and divert limited public safety assets from actual emergencies.
Public officials including lawmakers, judges and election workers are yet another primary target as part of an asymmetric political harassment and intimidation tool. This trend spiked dramatically during the 2024 election cycle when more than 50 separate swatting occurrences targeted members of the U.S. Congress, forcing municipal agencies to surge critical tactical and administrative resources to protect public figures from these hoaxes.[9]

Common Fabricated Scenarios

To ensure their hoaxes bypass standard call prioritization workflows, swatters will craft highly specific scenarios and scripts designed to force immediate emergency responses. Swatters frequently rely on falsifying violent and high casualty scenarios to generate a rapid, large-scale emergency response. These scenarios typically involve an active shooter, person with a weapon, a bomb threat, or a hostage situation.

Swatting attacks involving an active shooter or a person with a weapon are the most disruptive threat type, designed to immediately activate local tactical assault teams, regional mutual aid structures and immediate lockdown scripts. This form of swatting attack is used across all target types in a variety of situations.

Fabricated claims of explosives are intended to force chaotic building evacuations and hours of specialized sweeps. Reporting in 2025 pointed to an escalating trend of automated bomb threats explicitly targeting election tabulation offices to disrupt local democratic processes. In April 2026, a male subject called an elementary school claiming to have planted bombs in the trash cans, bushes and ceiling that were set to detonate. This was one of several successive swatting threats made to

5 Public Safety Threat Alliance (PSTA). "The Evolution of Swatting." Public Safety Threat Report. March 7, 2025.
6 Center for Internet Security (CIS) and Institute for Strategic Dialogue (ISD). "Purgatory Swatting Group Very Likely Responsible for False Active Shooter Reports at 10 U.S. Universities." Emerging Intelligence Report. August 27, 2025.
7 Northern California Regional Intelligence Center (NCRIC). "Suspicious Activity Report 2026-0008053-SAR." Partner Update Brief. May 6, 2026.
8 Northern California Regional Intelligence Center (NCRIC). "Suspicious Activity Report 2026-0007640-SAR." Partner Update Brief. April 1, 2026.
9 Center for Internet Security, Swatting Risk to Large Events and Mitigations (Center for Internet Security, June 2025).

schools in 2025 and 2026.[10]

Lastly, swatters will develop detailed narratives of armed and barricaded suspects holding multiple victims, potentially freezing scarce tactical and negotiation assets for extended periods of time. This tactic is frequently used against residents' homes, often targeting online gamers.

Tactics and Technologies Used by Swatters

The toolkits that contemporary swatters use have advanced far beyond standard burner phones or simple number blocking. Today's threat landscape features a sophisticated suite of virtual network infrastructure, AI voice-cloning, and live feed reconnaissance loops that deliberately exploit the structural vulnerabilities of our telecommunications and the natural inclination of a PST to believe the voice on the other end of the line.

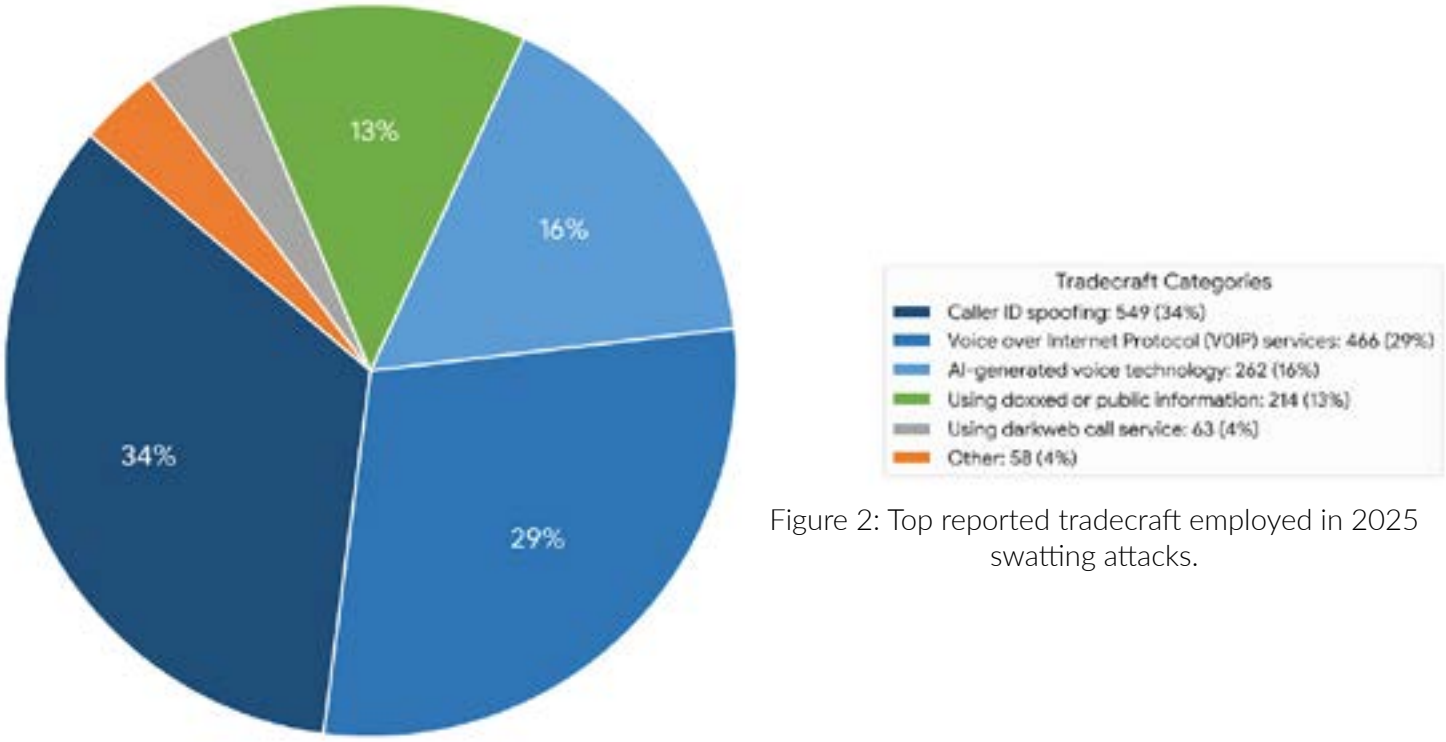

Figure 2: Top reported tradecraft employed in 2025 swatting attacks.

Caller ID Spoofing and Blocked Numbers

The technical foundation of a swatting call relies on manipulating the telecommunications signaling layer to overwrite authentic routing data. Attackers use spoofing software to alter the automatic number identification (ANI) profile displayed on the PST's console. In the survey, 549 respondents flagged caller ID spoofing as the number one barrier to verification. When a high-stakes call hits the queue displaying a neighbor's number or even the victim's own home landline, the PST is forced into an incredibly difficult guessing game, delaying standard traceback efforts.

10 https://www.facebook.com/boisecountysheriff/posts/press-releaseboise-county-sheriffs-officeapril-28-2026on-tuesday-afternoon-april/999987545743826/

VoIP Services

VoIP architecture is the primary engine behind high-volume, cross-jurisdictional swatting campaigns. Loose identity validation across virtual providers allows global threat actors to spin up and discard virtual numbers in seconds, a challenge noted by 466 respondents within the survey. Because these virtual lines operate completely detached from physical phone lines, PSTs cannot automatically isolate a physical location during a live crisis, eliminating the effectiveness of a call-back validation.

AI-Generated and Recorded Audio Signatures

We are seeing a major, dangerous shift in swatting tradecraft: the use of synthetic audio and high-fidelity sound injection. The APCO/PSTA swatting survey documented 262 instances where PSTs explicitly ran into AI-generated voice tactics, noting a signature robotic tone, flat cadence or unusual phrasing. Far more dangerous, however, is the injection of pre-recorded background audio loops. It is one thing to evaluate a suspicious caller, it is another entirely when your headset is flooded with the unmistakable sound of automated gun discharges, screaming victims or tactical reloading cycles, designed specifically to bypass a PST's skepticism and force an emergency dispatch. In March 2026, an attacker used an AI-generated voice to call police dispatch, demanding $10,000 and threatening to detonate a bomb if the ransom was not paid. The threat actor refused to provide personal information, and the caller ID was untraceable.[11]

Exploitation of Doxxed and Open-Source Personal Information (OSINT)

Before a threat actor ever dials an emergency line, they routinely conduct detailed reconnaissance on their target using open-source intelligence (OSINT) strategies. Perpetrators harvest personal indicators from underground illicit data dumps, active social media accounts and public commercial data brokers. This reconnaissance package typically includes family members' names, workplace rosters, specific

11 Northern California Regional Intelligence Center (NCRIC). "Suspicious Activity Report 2026-0000512-SAR." Partner Update Brief. March 18, 2026.

residential architectural layouts and local police jurisdictional designations. By weaving these authentic personal details directly into their emergency dialogue, swatters deceive the PST into believing the caller has immediate, firsthand visual proximity to the fabricated crime scene, dramatically shortening the time available for analytical verification.

Use of Online Platforms, Encrypted Communications and Anonymization Tools

The contemporary swatting landscape has transformed from decentralized individual actors into a highly structured, commercialized "swatting-as-a-service" economy. Prolific online groups—such as the "Purgatory" group, the "Kirk Mafia" and the extremist online collective known as "764"—coordinate regional campaigns through encrypted channels like Telegram. These actors manage automated marketplaces and underground bots, allowing clients to purchase a full "school closure" or an armed tactical residential deployment for a nominal cryptocurrency fee that can average $50 to $75 USD. To hide their footprints, threat actors pass data packets through multi-layered virtual private networks (VPNs) with strict no-logging policies, Tor onion-routing configurations, and residential proxy networks that mimic regular domestic internet subscribers, rendering real-time tracking almost impossible during an active event.

Operational Challenges to Verification and Response

The convergence of techniques such as spoofed caller ID tracking numbers, virtual VoIP network routing paths, voice synthesis tools and background audio loops introduces intense friction to frontline officers. Operating under a strict "no-fail" mandate, PSTs must treat every incoming report as completely valid until definitive proof of a hoax is established. The severe psychological toll of processing a call flooded with gunfire sounds while verifying manipulated phone numbers collapses the PST's available processing time, forcing a pragmatic decision favoring rapid tactical dispatch over unrealistic forensic research.

Swatting as a Cyber-Physical Threat

Viewing swatting strictly through the lens of a digital problem ignores the physical peril it introduces into our neighborhoods. By treating these incidents as cyber-physical threats, we expose the reality that a malicious VoIP call originating in the cyber domain from anywhere across the globe has direct impacts in the physical domain, forcing first responders and innocent citizens into high-risk situations.

For public safety agencies, cybersecurity incidents like ransomware or web defacements and dispatch operations are two separate worlds. Swatting shatters that division. It is a textbook cyber-physical threat where an anonymous global attacker leverages digital tools to force immediate, high-risk physical outcomes in the real world.

> *"It is a textbook cyber-physical threat where an anonymous global attacker leverages digital tools to force immediate, high-risk physical outcomes in the real world.*

When cybercriminals utilize a dark web service or an encrypted Telegram group to mask their identity, the technical exploit does not stop at the console screen. A digital data packet sent from a proxy server thousands of miles away can instantly translate into heavily armed tactical teams rolling down a quiet local street with emergency lights and sirens. The ECC is no longer just handling a phone call, it is processing the front end of a multi-layered technical hack designed to manipulate physical infrastructure and law enforcement's response.

This technical reality shifts how we view our personnel. The PST console is no longer just a routing switchboard, it operates as an active threat intelligence outpost. The PST is the human firewall tasked with decoding, filtering and validating complex adversarial data streams under intense time constraints.

Every shift, PSTs are forced to evaluate each and every call for assistance. A PST must listen closely to determine if the screaming voice in their headset is a real person in distress, or an AI-generated synthetic voice intended to mimic human panic. They must cross-reference caller ID data knowing that VoIP technology easily allows global attackers to spoof a victim's actual residential line or a known contact to manufacture false credibility. The critical diagnostic assessments that a PST makes during the opening seconds of a call dictate whether field units roll up with weapons drawn or approach with calculated caution. This places the PST as the primary line of defense inside modern public safety risk management.

Integration of Swatting into Public Safety Risk Management

Adopting a cyber-physical risk framework allows ECC directors to evolve their operational planning from a reactive posture to a more proactive defense. Rather than treating swatting as an unresolvable series of annoying prank calls, leadership can engineer robust, cross-functional mitigation strategies recommended by national authorities like the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS) and state fusion centers[12]:

- Pre-crisis verification loops: Directors should establish real-time collaboration channels between PSTs and community stakeholders such as local school administrators and corporate security managers. Building these verification loops allows PSTs to rapidly check the ground-truth situation at a facility before deploying an aggressive, heavily armed tactical force.
- Targeted dispatch screening scripts: Following models from regional intelligence centers, ECCs should integrate specific, analytical questioning protocols into their training academies. Training PSTs to press for hyper-granular physical details about a location or the individuals involved helps expose the inconsistencies of a remote swatter relying on static OSINT.
- Public information and personal data hygiene: Aligning with federal infrastructure recommendations, public safety entities must actively educate potential targets on how to secure their personal information online. Reducing the online footprint of local public officials, corporate employees and citizens minimizes the open-source data swatters can harvest to build high-credibility call scripts.

Training, Policy and Coordination

Training, policy and coordination remain foundational yet unevenly implemented components of public safety efforts to prevent and mitigate swatting incidents. Survey findings indicate that the availability of swatting specific training is inconsistent across ECCs, with many agencies reporting limited or no formal instruction addressing the unique indicators, technologies and decision making challenges associated with swatting events. Where training does exist, its effectiveness is often dependent on local initiative rather than standardized curriculum, resulting in wide variability in preparedness.

As swatting tactics increasingly rely on caller ID spoofing, VoIP infrastructure, synthetic audio and detailed OSINT exploitation, the absence of structured, scenario based training places PSTs at a disadvantage when attempting to differentiate legitimate emergencies from deliberate deception

12 https://www.ic3.gov/CSA/2024/240529.pdf

under time critical conditions.

PST confidence levels reflect this disparity in training and preparedness. PSTs operating in ECCs with dedicated swatting training or recurring in-service exercises report greater confidence in applying analytical questioning techniques, identifying inconsistencies in caller narratives, and escalating concerns through supervisory and verification channels. In contrast, PSTs in ECCs without such training frequently report uncertainty when faced with highly specific or emotionally manipulative calls, particularly those designed to exploit a “no fail” emergency response culture. This confidence gap has direct operational implications, as the initial assessment and classification of a call often determines the scale, speed and posture of the field response.

The survey also reveals a substantial operational gap in the form of absent or informalized SOPs. A significant number of ECCs report having no written swatting specific SOPs to guide call handling, verification steps, supervisory notification or coordination with responding agencies. In the absence of formal policy, responses to suspected swatting incidents are often dependent on individual experience or shift-level practices, increasing the likelihood of inconsistent outcomes. This lack of documentation further complicates post incident reporting, trend analysis and the development of institutional knowledge necessary to address repeat or multi jurisdictional campaigns.

Effective coordination with law enforcement and external partners is a critical mitigating factor, yet it remains underutilized in many jurisdictions. ECCs need to develop pre established coordination mechanisms with local law enforcement, tactical units, school officials, corporate security teams, state homeland security offices and fusion centers. ECCs that have implemented shared verification protocols and trusted points of contact are better positioned to validate high risk calls and identify emerging patterns across jurisdictions. Without such coordination, swatting incidents are often managed as isolated events, allowing serial offenders to exploit jurisdictional boundaries and operational silos. Strengthening cross disciplinary coordination enhances situational awareness, supports safer response strategies and reduces the likelihood that malicious cyber enabled calls result in unnecessary or dangerous real-world deployments.

Challenges in Tracking and Reporting

A significant advantage held by modern swatting syndicates isn’t their digital toolset; it is our own institutional fragmentation. When individual ECCs handle these highly coordinated multi-jurisdictional exploits in localized silos, short-staffed and without written SOPs, we inadvertently protect the threat actors from the centralized, macro-level intelligence tracking needed to help mitigate this threat.

The primary technical challenge in countering swatting behavior remains the complexity of real-time trace operations across interconnected digital telecommunications pathways. Attackers pass calls through international gateway points, virtual server infrastructure and complex session initiation protocol (SIP) paths. This multi-carrier obfuscation completely blocks real-time technical location tracing during the active phase of an incident.

> *"One of our biggest national vulnerabilities isn't the technology the swatters use; it's how we collect threat intelligence.*

One of our biggest national vulnerabilities isn't the technology the swatters use; it's how we collect threat intelligence. A plurality of survey respondents (277 respondents) stated that no centralized authority or external agency tracks their ECC's swatting data. While 598 respondents report incidents to local investigators after the scene is cleared, and smaller segments notify the FBI (152 respondents) or state Homeland Security teams (99 respondents), there is no mandatory, uniform national platform to log these events and then access them for analysis. This fragmented system creates a massive blind spot as a serial swatter can hit five neighboring counties using the exact same virtual number and technical signature, and none of those ECCs will connect the dots until after tactical units are already on scene. This is why 445 survey respondents identified a unified national threat database as a strategic necessity.

Beyond lacking a centralized database, there is currently no uniform definition for swatting applied consistently across municipal, county and state public safety agencies. These occurrences are frequently cataloged under generic, broad dispatch event descriptions such as "false alarm," "misuse of emergency lines" or "terroristic harassment." This inconsistent record-keeping obscures the true frequency of the threat and makes it extremely difficult for analysts to recognize a single, coordinated campaign targeting multiple regions simultaneously.

Finally, we must look closely at our internal support structures. ECCs face severe, long-term staffing and retention challenges. When the ECC floor is short-staffed and calls are stacked up, PSTs must focus entirely on the next calls in the queue, meaning detailed technical logging and post-incident reporting fall by the wayside. PSTs routinely experience high-stakes, technology-driven confrontations relying on nothing but ad-hoc instincts and on-the-job learning, a gap that presents a significant operational vulnerability for public safety leadership and the communities they serve.

Needs and Recommendations

Survey findings clearly demonstrate the need for standardized policies and written SOPs specific to swatting incidents in emergency communications. Establishing standardized policies and SOPs would provide a common framework for analytical questioning, enhanced verification steps, supervisory notification, and coordination with responding units, thereby reducing variability in response during high-risk incidents.

The survey also highlights a direct relationship between training availability and PST confidence levels, underscoring the need for enhanced training for both PSTs and supervisors. Respondents from agencies that included swatting scenarios in academy or in-service training reported greater confidence in identifying suspicious indicators and managing complex, technology-enabled deception. Scenario-based training that reflects contemporary swatting tactics, including spoofed caller identification, VoIP services, synthetic audio, and OSINT exploitation, would help close this confidence gap and support more consistent decision-making during critical call intake.

Survey responses further indicate a need for improved verification and call-handling tools to support PSTs during suspected swatting events. Enhancing call-handling workflows through structured verification processes, decision support tools and access to trusted secondary verification contacts can help PSTs assess credibility more effectively without delaying legitimate emergency response.

The findings also point to gaps in interagency coordination and information sharing. Strengthening pre-incident coordination and establishing shared communication pathways with law enforcement leadership, school officials, corporate security teams, and regional intelligence partners would improve situational awareness and support faster identification of coordinated or repeat activity.

Improved tracking and reporting practices emerged as a critical need across survey responses. Developing standardized reporting criteria and encouraging participation in centralized or regional tracking mechanisms would support more accurate data collection, trend analysis and intelligence sharing. Improved tracking not only enhances local operational awareness but also strengthens the public safety community's ability to address swatting as a persistent and evolving threat.

Conclusion

Swatting presents a sustained and evolving challenge with clear operational and safety implications for PSTs, responding agencies and the communities they serve. Swatting incidents routinely exploit emergency systems to trigger armed law enforcement responses, large scale evacuations, and service disruptions placing responders, victims and bystanders at unnecessary risk. The psychological toll on PSTs and fellow first responders, combined with the diversion of limited public safety resources, underscores the seriousness of swatting as more than a nuisance or isolated misuse of emergency services.

Addressing this threat requires public safety agencies to confront both current operational gaps and emerging technological risks. Survey findings reveal persistent deficiencies in training, written policies, verification tools, coordination, and tracking practices. As swatting tactics increasingly leverage sophisticated cyber techniques such as caller ID spoofing, VoIP services, synthetic audio and coordinated online activity, these gaps will continue to widen without deliberate action.

ECC leaders, policymakers and public safety partners need to take coordinated, proactive steps to mitigate swatting risks. Treating swatting as a cyber-physical threat demands investment in standardized policies and procedures; enhanced and recurring training for PSTs and supervisors; improved call handling and verification capabilities; and stronger interagency collaboration across law enforcement, cybersecurity, telecommunications and intelligence communities. By strengthening preparedness and coordination, ECCs can reduce the likelihood that malicious digital deception results in dangerous real-world consequences, and they can reinforce the resilience, safety and trust placed in emergency communications systems.

Sources may use TLP:GREEN when information is useful for the awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community. If the community is not specified, assume the cybersecurity/defense community.
https://www.cisa.gov/tlp

APCO International

Leaders in Public Safety Communications®

apcointl.org

PSTA

Public Safety Threat Alliance

Public Safety ISAO

motorolasolutions.com/psta