United States – August 22, 2025

Trend Analysis - Understanding the Evolving Risk Landscape of Swatting Threats and Their Expanding Impact on Business, Government, and Public Institutions

Contact: GlobalInsightsTeam@everbridge.com

Overview

On August 21, separate and unrelated false reports of active shooter threats at both Villanova University in Pennsylvania and the University of Tennessee at Chattanooga prompted significant law enforcement responses and temporary campus lockdowns. While both incidents were ultimately confirmed as hoaxes, they illustrate a broader pattern of swatting activity, in which individuals deliberately report false emergencies with the intent of prompting a tactical law enforcement response. Once regarded primarily as isolated acts of harassment, swatting has become an increasingly disruptive threat to educational institutions and workplaces across the U.S. Recent high-profile cases have demonstrated the substantial operational disruption, psychological strain, and reputational consequences these incidents can cause. As swatting becomes more frequent and complex, institutions are under growing pressure to strengthen how they verify and respond to potential threats.

Trend

Swatting activity has evolved considerably over the past decade, moving from niche online harassment to a persistent and operationally disruptive threat. Two key trends characterize this shift: first, the expansion of swatting targets beyond its origins in gaming and K–12 schools to include higher education, workplaces, government facilities, and political figures; and second, the growing technical sophistication used to execute these hoaxes.

Initially rooted in online gaming culture, swatting began as a means of harassment in which individuals called in fabricated emergencies to disrupt livestreams or retaliate against rivals. The tactic then gained traction across the U.S. education sector, particularly in K–12 schools, which experienced a surge in false active shooter threats between 2018 and 2023. In 2025, the pattern of targeting has shifted further. The false active shooter reports at Villanova University and the University of Tennessee at Chattanooga on August 21 reflect swatting's spread into higher education. Earlier in the year, Claremont McKenna College in Southern California was similarly affected by a fabricated bomb and hostage threat, resulting in a multi-agency response and extended disruption.

Beyond educational institutions, swatting has increasingly been used to target individuals in positions of public authority. On July 4, police responded to a hoax emergency call alleging an armed child at the home of a senior U.S. Secret Service official. Just weeks earlier, Romanian national Thomasz Szabo pled guilty to orchestrating a transnational swatting and bomb-threat campaign that included threats against a former U.S. president, sitting members of Congress, and federal buildings. Szabo used encrypted platforms and caller anonymization tools to direct threats from abroad, which complicated attribution and enforcement. These cases show how swatting has become not only a tool of disruption but also one of intimidation, extending beyond institutional settings into private residences and across national borders.

In parallel, the technical methods used to carry out swatting have become increasingly sophisticated. Perpetrators now regularly use caller ID spoofing, voice modulation software, internet-based calling services, and pre-recorded sound effects such as gunfire to increase the realism of their hoaxes. The widespread availability of anonymization tools has lowered the barrier to entry, allowing juveniles, domestic extremists, and international actors to launch high-impact incidents with relatively little risk of detection.

The expansion of swatting targets and the increasing sophistication of hoax tactics confirm that swatting has matured into a durable and adaptive threat that is no longer confined to a single platform, institution, or motive. As this evolution continues, understanding the specific vulnerabilities that make certain institutions more susceptible to disruption is critical for assessing operational risk and anticipating future developments.

Risk

Although swatting incidents are based on fabricated threats, the emergency responses they provoke carry real operational risk. Law enforcement is often deployed before a threat can be confirmed, resulting in major disruptions and introducing safety concerns in environments that may be unprepared for rapid crisis escalation. Evacuations, lockdowns, and tactical clearances can lead to physical injuries, trigger panic, and cause psychological distress, particularly among individuals who believe they are facing a genuine threat. In volatile or crowded settings, there is also the risk of misidentification, inappropriate use of force, or confrontations that escalate unnecessarily.

Academic institutions remain highly vulnerable due to their physical layouts and public accessibility. Open campuses, multiple entry points, and decentralized facilities hinder swift threat assessment and containment. During high-density periods such as orientation, exams, or public events, these vulnerabilities increase. While emergency alert systems are critical for life safety, they can amplify confusion and alarm if deployed without sufficient clarity. Poorly managed incidents may invite criticism from students, parents, or the media and can reduce stakeholder confidence in overall campus safety.

Swatting directed at public officials and other high-profile individuals introduces a distinct set of risks. When law enforcement responds to a hoax involving a private residence or family member, it often does so with limited situational awareness and an elevated posture. In these cases, the margin for error is small. A misjudged response can lead to reputational fallout, physical harm, or broader political consequences. These risks are compounded when incidents intersect with themes of political extremism or harassment.

Private-sector organizations face growing exposure as swatting tactics increasingly target corporate environments. A single fabricated threat directed at a company headquarters, regional office, or logistical facility can force evacuations, halt operations, and disrupt continuity. Interruptions to critical services or data infrastructure may also draw regulatory scrutiny or diminish investor confidence. In customer-facing sectors, reputational harm is a core concern, especially if emergency responses are seen as excessive or poorly coordinated. Remote and hybrid workforces further complicate emergency procedures, with decentralized teams facing inconsistencies in local law enforcement engagement and internal communication. Additionally, swatting increasingly overlaps with cyber risks, as threat actors exploit leaked credentials or internal planning data to enhance the realism and impact of their hoaxes.

Technology continues to magnify these challenges. Swatting actors routinely use spoofed caller IDs, encrypted communication tools, and internet-based services to obscure attribution. Many incidents include realistic audio effects such as simulated gunfire or distress sounds to heighten urgency and delay dismissal. As a result, institutions are often forced to treat reports as credible until proven otherwise, triggering full-scale responses even in the absence of an actual threat.

Resilience

Limiting organizational exposure and improving threat recognition processes represent the most effective early-stage measures against swatting incidents. Businesses, particularly those with public-facing operations or high-profile personnel, can reduce their visibility to threat actors by auditing and restricting access to sensitive information such as staff directories, executive itineraries, facility layouts, and internal contact structures. Educational institutions and government offices may similarly minimize risk by controlling the public availability of building maps, schedules, and personal identifiers. Technology can also play a central role in early threat identification when embedded into broader security operations. Caller authentication systems, voice analytics tools, and behavioral anomaly detection software may assist in flagging suspicious communications prior to response escalation. Equipping frontline personnel with this awareness strengthens an organization’s ability to assess threats before escalation. By identifying potential hoaxes early, institutions are better positioned to avoid unnecessary disruption and activate a proportionate, informed response if a swatting incident does occur.

In the event that a swatting threat is reported, organizations require a clear and scalable response framework to support timely decision-making. Tiered protocols can help distinguish between low-credibility reports and those that appear more immediate or specific, enabling security teams to escalate proportionally, using access restrictions or limited lockdowns while internal verification is underway. Maintaining control during a swatting incident depends in part on well-defined internal communication protocols that ensure clarity, consistency, and rapid information flow. Pre-scripted messaging tailored to different alert levels can reduce confusion and provide timely, consistent updates. Public-facing organizations may prepare external communications in advance to ensure message discipline during an active incident. Continuity measures such as remote access activation, alternate site operations, or delayed work start procedures can help preserve business functions during a disruption. Sectors with regulatory or logistical sensitivities, such as finance, healthcare, or distribution, may preposition backup workflows or offsite processing capabilities as part of broader contingency planning.

Effective post-incident recovery relies on structured review processes that assess operational performance and identify points of failure. After-action assessments involving all relevant departments can surface delays in response, coordination breakdowns, and deficiencies in escalation protocols. For businesses, such evaluations may include analysis of legal exposure, brand impact, and insurance considerations following a public or disruptive event. Educational institutions may use incident reviews to refine collaboration with law enforcement and reassess communication procedures for students, faculty, and parents. Public officials may consider operational security enhancements or digital footprint minimization following repeat targeting. Across all sectors, the emphasis remains on learning and institutionalizing improvements. As swatting tactics continue to evolve, organizations that internalize the threat as an ongoing operational concern, rather than a one-off disruption, will be better positioned to respond decisively and preserve continuity.