PUNCH RESCUE

Building Strong Emergency Infrastructure: A Practical Guide for School Safety Leaders

COVERING:

What We've Learned About Emergency Communication

Why Infrastructure Resilience Matters

How to Evaluate Solutions That Work

Q1 2026

Inside This White Paper

Emergency communication systems are facing a serious challenge. Far too often, the conditions under which they are needed most are often the very conditions in which they are most likely to fail.

This whitepaper examines what school safety experts have learned about emergency communication infrastructure. The aim of this examination is not to dwell on tragedy, but to understand the patterns that can inform better decisions. We draw on official investigations, commission reports, and documented findings to make the case for infrastructure-first solutions. We looked for systems designed to function when both when things are running smoothly and when conditions take a turn for the worse.

For school leaders, the need for consistent, reliable performance is not theoretical. It directly affects preparedness, defensibility, and accountability.

What We Cover:

- Patterns identified across emergency response research: what tends to fail, and why
- Technical realities of infrastructure dependencies: power, networks, and notification systems
- Human factors science: why simplicity under stress is a functional requirement
- Regulatory landscape: Alyssa's Law and compliance requirements across states
- Evaluation framework: questions to ask when assessing any solution
- Practical implementation: what infrastructure-first solutions look like, including Punch Rescue’s platform

Key Findings:

Official investigations into major school emergencies have consistently identified communication breakdowns as contributing factors in emergency response challenges. These breakdowns often follow predictable patterns documented in commission reports and after-action reviews:

- *Radio communication systems have experienced "throttling" during high-demand incidents, blocking critical transmissions.*
- *Building construction can significantly impair radio signals. Some responders have reported radios "did not function" inside school buildings.*
- *Notification delays measured in hours have contributed to response challenges.*
- *Network congestion during high-demand moments can block or delay critical messages.*

- *Power dependencies create single points of failure.*

Research from psychology and human factors engineering explains why complex interfaces fail under stress. Often, cognitive capacity shrinks, fine motor skills deteriorate, and people revert to trained habits. Rather than simply revealing some kind of training problem, these issues exhibit normal human physiology.

Alyssa's Law and related legislation is spreading across the United States, reflecting a growing recognition that emergency communication requires dedicated investment and clear standards.

What This All Comes Down To:

Organizations responsible for the safety of large groups of people should evaluate emergency communication systems based on their resilience under degraded conditions. It does not help to observe their performance under ideal conditions. Hardware-integrated, network-independent solutions are designed to address documented failure modes in ways that software-only approaches often cannot.

This paper provides the framework and evidence to support that evaluation process, along with a detailed look at how Punch Rescue's platform implements these principles in practice.

Starting with The Infrastructure Question

When evaluating emergency communication systems, most comparisons focus on features: notification channels, integration counts, response time claims. These metrics assume that the underlying infrastructure (power, network connectivity, device availability) will function normally during an emergency.

This assumption deserves scrutiny.

Real emergencies can create cascading infrastructure challenges. Power outages eliminate Wi-Fi. Network congestion can block cellular calls. Stress disrupts cognitive function. The difference between a demonstration performance and crisis performance is worth understanding, because that is where reliability is best measured.

A Different Way to Evaluate

This whitepaper argues that organizations responsible for the safety of large groups of people should focus on evaluating emergency communication systems based on their resilience under degraded conditions.

We are not the first to make this argument. The broader school safety community has been moving in this direction for years, informed by post-incident research, regulatory developments, and the practical experience of safety directors. Many of these directors have seen the difference between systems that work on paper and systems that work in practice.

What we offer here is a synthesis of our learning, organized into a framework that can guide decision-making.

What This Document Provides

- Patterns from emergency response research: what the safety community has learned about communication system failures
- Technical analysis of infrastructure dependencies: understanding what your current systems rely on
- Human factors science: why simplicity is a functional requirement
- Regulatory overview: Alyssa's Law and compliance requirements by state
- Evaluation framework: questions to ask when assessing any emergency communication solution
- Practical application: how these principles translate into real systems, including our own Punch Rescue platform

Our Perspective

We are a company that builds emergency communication infrastructure. We have a point of view, and we're transparent about it. We believe hardware-integrated, network-independent solutions can better address many documented challenges of emergency communication than software-only alternatives, or more fragile network-dependent hardware.

That said, this paper is designed to be useful regardless of which solution you ultimately choose. The evaluation framework we provide applies to any vendor. The questions we suggest asking apply to our competitors as much as to us. Our goal is to raise the standard of the conversation. We believe better-informed buyers make better decisions, and better decisions improve outcomes.

If you read this paper and decide our approach isn't right for your organization, we will still have succeeded if you make that decision based on the right criteria.

Lessons from the Field

The school safety community has learned difficult lessons over the past two decades. Official investigations, commission reports, and after-action reviews have identified patterns in how emergency communication systems perform under real-world conditions.

We approach this topic with humility and deep respect for the victims, survivors, and families affected by these tragedies.

What follows are the patterns that emerge across multiple incidents and research studies. These patterns are drawn from official reports and publicly documented sources, presented as lessons for future preparedness. These are not case studies meant to be endlessly dissected.

Documented Incidents and Their Lessons

The incidents we reference here have been extensively investigated by government agencies, independent commissions, and law enforcement bodies. We draw exclusively from official reports and publicly documented findings.

Parkland, Florida (2018): Radio System Overload

The shooting at Marjory Stoneman Douglas High School on February 14, 2018, killed 17 students and staff. The MSD High School Public Safety Commission conducted an extensive investigation and issued comprehensive reports documenting response challenges.

Documented Communication Failures:

The county's radio system experienced "throttling"—a condition where too many users causes blocking or delays. Commission testimony documented that "many first responders did not receive radio transmissions at all because the amount of radio traffic overloaded the system."

Dispatchers reported officers "could hear nothing, just complete silence, because nobody was able to get on the radio."

Officers from different agencies could not communicate effectively due to separate, incompatible radio systems. Some officers resorted to hand signals when radios failed.

Source: Marjory Stoneman Douglas High School Public Safety Commission Reports (2019-2024); Sun-Sentinel reporting on commission testimony.

Uvalde, Texas (2022): Command and Coordination Breakdown

On May 24, 2022, a gunman killed 19 students and two teachers at Robb Elementary School. The Department of Justice conducted a Critical Incident Review, resulting in a nearly 600-page report released in January 2024.

Documented Communication Failures:

The school district police chief, identified as the de facto incident commander, "discarded his radios during his arrival thinking they were unnecessary."

The DOJ found "cascading failures of leadership, decision-making, tactics, policy, and training" with communication breakdowns at multiple levels. Leadership "demonstrated no urgency for establishing a command and control structure, which led to challenges related to information sharing."

Some responders reported that radios did not function inside the building due to construction materials blocking signals.

Source: U.S. Department of Justice Critical Incident Review (January 2024); Rockefeller Institute analysis.

Virginia Tech (2007): Notification Delays

On April 16, 2007, a shooter killed 32 students and faculty in two separate attacks. Governor Tim Kaine appointed a Review Panel to investigate, which documented significant notification delays.

Documented Communication Failures:

The first shooting occurred at approximately 7:15 AM. The first campus-wide email alert was not sent until 9:26 AM. That was more than two hours later.

The Review Panel found the university police "erred in not requesting that the Policy Group issue a campus-wide notification." The alert that was sent was not specific. It did not state a gunman was at large.

The second attack began at approximately 9:40 AM, after the delayed alert was sent but before many had seen it.

Source: Virginia Tech Review Panel Report (August 2007).

Apalachee High School, Georgia (2024): Infrastructure That Worked

On September 4, 2024, a shooting at Apalachee High School killed two students and two teachers. This tragic incident also demonstrated how emergency communication infrastructure can support faster response when systems are in place.

Documented Successes:

Teachers had been issued wearable panic badges approximately one week before the incident. Multiple staff members activated panic buttons, triggering immediate lockdown alerts and law enforcement notification.

Sheriff Jud Smith reported "over 20 alerts from people in that general area" that helped responders locate the incident. A teacher reported his smartboard displayed "hard lockdown" before he heard gunshots, giving critical preparation time.

The suspect was in custody within six to seven minutes of the first alert.

Georgia Bureau of Investigation Director Chris Hosey stated the system "prevented this from being a much larger tragedy." Former FBI Agent Brad Garrett noted the panic buttons "probably saved a lot of lives."

Source: ABC News, NBC News, CNN coverage (September 2024); Georgia Recorder.

Pattern 1: Communication Networks Can Become Overwhelmed

When emergencies occur, communication demand spikes dramatically. Everyone (staff, students, parents, responders, media) attempts to communicate simultaneously. This surge can overwhelm networks designed for normal operating conditions.

Post-incident research has documented instances where:

- Radio systems experienced severe capacity constraints, blocking or delaying transmissions.
- Cellular networks experienced significant call congestion during peak demand.
- Responders resorted to cell phones, text messages, or physical runners when primary communication failed.
- Critical information failed to reach decision-makers due to network overload.

The Parkland commission documentation provides a clear example. When the radio system became overloaded, "many first responders did not receive radio transmissions at all." This is not a hypothetical concern. It is a documented reality from a major incident.

Telecommunications providers and public safety experts have publicly noted that consumer networks are not designed for extreme surge scenarios. In other words, in a large-scale emergency, the "normal" network may not behave normally.

The Lesson: Emergency communication systems should not rely solely on networks that will be competing with surge traffic during the moments they're needed most. Dedicated, independent communication pathways provide resilience that shared networks cannot.

Pattern 2: Building Construction Can Block Signals

Modern building construction—concrete, steel, energy-efficient windows—can significantly impair radio and cellular signals. What works in a parking lot may not work inside a classroom.

The Uvalde DOJ report documented that some responders experienced radio communication failures inside the building due to construction materials blocking signals. This is a recurring challenge in after-action reports.

Other documented examples include:

- Radio signals that failed to penetrate school buildings due to construction materials
- Responders who knew from prior experience that their radios would not work inside certain buildings
- "Dead zones" in basements, stairwells, and interior rooms where signals could not reach
- Coordination failures when commanders could not communicate with teams inside buildings

The Lesson: In-building coverage cannot be assumed. Systems should be designed with repeaters or mesh networks that ensure signals reach every room (even areas lacking reception).

Pattern 3: Notification Delays Can Have Significant Consequences

Speed matters in emergency notification. The Virginia Tech Review Panel documented a notification delay of over two hours between the first shooting and the first campus-wide alert. The second attack began shortly after the delayed alert was sent but before many had seen it.

Contributing factors to notification delays documented across incidents have included:

- Uncertainty about whether a situation warranted emergency notification
- Multi-step approval processes before alerts could be sent

- Limited notification channels that could not reach all affected populations quickly
- Systems that required someone to be at a specific location (like a front office) to initiate alerts

In contrast, the Apalachee incident demonstrated the value of distributed activation capability. Multiple staff members were able to activate alerts immediately from their locations, triggering building-wide lockdown and law enforcement notification within moments.

The Lesson: Emergency notification should be initiable from anywhere by authorized personnel. It should not be dependent on reaching a specific location or navigating complex approval processes. Distributed activation capability reduces delay.

Pattern 4: Interoperability Challenges Affect Coordination

Emergency response often involves multiple agencies, including school staff, local police, county sheriff, fire department, EMS. When these groups use incompatible communication systems, coordination suffers.

The Parkland commission documented that officers from different agencies operated on incompatible radio channels, creating coordination challenges. The Uvalde DOJ report noted that communication breakdowns occurred at multiple levels, affecting unified command.

Research has documented situations where:

- Different agencies operated on incompatible radio channels.
- Critical information shared on one channel never reached responders on another.
- Unified command was delayed because agencies could not communicate effectively.
- Duplicate or conflicting information circulated because there was no common operating picture.

The Lesson: Emergency communication systems should support integration with first responder workflows. This involves providing location data, alert status, and coordination capabilities that can function across agency boundaries.

Pattern 5: Technology Alone Does Not Guarantee Results

Having emergency technology installed is not the same as having emergency capability. This is perhaps the most important pattern revealed. Systems that exist on paper may fail in practice if they are not regularly tested, if staff are not trained, or if the technology has limitations that only become apparent under stress.

The Uvalde incident documented a case where a school district police chief discarded his radios "thinking they were unnecessary." This decision severely impaired coordination. This speaks to both training gaps and the importance of building reliable habits around emergency tools.

After-action reports have noted:

- Emergency plans that had not been tested with realistic drills
- Staff who were unfamiliar with emergency systems because they were rarely used
- Technology that worked during demonstrations but failed under real conditions
- Complex interfaces that overwhelmed users when cognitive capacity was already depleted by stress

The Apalachee incident provides a counterexample. Teachers had received wearable panic devices approximately one week before the shooting. When the emergency occurred, multiple staff members activated them immediately. This suggests that even limited familiarity with simple, wearable devices can translate to effective use under stress.

The Lesson: Effective emergency infrastructure requires ongoing investment in drills, training, and testing. Systems should be simple enough that stressed users can operate them, and familiar enough that staff default to using them correctly.

The Importance of Real-Time Awareness

One of the most significant lessons from documented emergency responses is the critical importance of real-time situational awareness. When responders and administrators know exactly where people are, which devices are functioning, and what alerts have been triggered, they can make better decisions faster.

At Apalachee, Sheriff Jud Smith reported that "over 20 alerts from people in that general area" helped responders understand the scope and location of the incident. This real-time information contributed to the rapid response. The suspect was in custody within six to seven minutes.

Consider the alternative. If administrators cannot see device status in real time, they may discover during an emergency that critical devices have dead batteries, repeaters have gone offline, or coverage gaps exist in key areas.

Without real-time visibility:

- A teacher's panic device with a dead battery fails when needed, but no one knew it was non-functional.
- A repeater in a basement goes offline, leaving staff in that area without coverage. Administrators remain unaware.
- During a fire evacuation, administrators cannot confirm whether all staff have exited because they have no visibility into personnel locations.

Real-time awareness should provide:

- Device status monitoring: Live visibility into every device's status (online or offline, battery level, last communication). Administrators should receive proactive alerts when devices go offline.
- Location awareness: During an emergency, knowing where people are located is critical. Real-time location tracking allows responders to navigate directly to alerts and enables post-evacuation accountability.
- Alert visibility: When an alert is triggered, the system should immediately display who triggered it, from where, and what type.

This is a requirement for defensible preparedness. How can you demonstrate due diligence if you cannot prove your system was functional at the time of an incident?

Synthesis: Designing for Degraded Conditions

These patterns, drawn from official investigations and documented findings, point toward our design philosophy. Emergency communication systems must be designed for degraded conditions, not ideal ones.

This means:

- Network independence: not relying solely on infrastructure that may be overwhelmed
- Building-wide coverage: making sure signals reach every room, including areas with poorer reception
- Distributed activation: allowing alerts from anywhere, beyond fixed locations
- Interoperability: supporting coordination with first responders across agency boundaries
- Operational simplicity: working within the cognitive constraints of stressed users
- Real-time visibility: providing administrators with continuous awareness of system status and personnel location

The rest of this paper explores these principles in detail. We examine the technical realities, the human factors, science, the regulatory landscape, and ultimately, what solutions that embody these principles look like in practice.

Hidden Infrastructure Dependencies

Even well-equipped schools often overlook critical dependencies in their emergency communication systems. Understanding what your current systems rely on is the first step toward evaluating whether those dependencies create unacceptable risks.

This section examines common failure points (such as power, network connectivity, and third-party notification services). It also explains what "degraded conditions" mean in practice.

Many of these dependencies are characteristics of shared infrastructure under stress, such as power grids, public networks, consumer devices, and cloud services.

Power Dependency

Traditional alarm panels, intercoms, PA systems, and Wi-Fi access points all require electricity. During a power outage (whether it's caused by weather, accident, or deliberate action), a school without backup power at every layer can lose critical communications.

The Hidden Reality

If a panic button app relies on the school's Wi-Fi network, a power loss may render it ineffective. Routers and access points can go offline quickly. Standard Wi-Fi equipment often has no battery backup unless it's specifically equipped with uninterruptible power supplies. Backup duration can vary widely.

Many schools have backup generators for essential systems, but "essential" often means HVAC and lighting. It does not necessarily include network infrastructure. Even where network backup exists, it may cover core switches but not every access point in every classroom.

What Infrastructure-First Solutions Do Differently

Hardware-integrated emergency systems address power dependency by building battery backup into the devices themselves. Wearable panic devices can operate on battery power independent of building electricity. Repeaters and base stations can include backup power designed to maintain operation during outages.

Punch Rescue's platform, for example, uses devices designed for long-life battery operation with replaceable batteries. This reduces daily charging requirements and supports continuity during building power disruptions.

Wi-Fi and Local Network Dependency

Many emergency notification solutions, particularly app-based and IP phone systems, depend on the school's local network or Wi-Fi. This creates several vulnerabilities.

Coverage Gaps

Wi-Fi may not cover all areas of a campus. Basements, outdoor fields, portable classrooms, stairwells, and maintenance areas often have weak or no signal. An emergency that occurs in a coverage gap may not be reportable through Wi-Fi-dependent systems.

Bandwidth Saturation

During emergencies, network usage spikes. Students streaming news coverage, staff attempting video calls, security cameras uploading footage... all these compete for bandwidth. If an emergency alert relies on that same network, it may lag or fail to deliver.

Single Point of Failure

If the network core goes down from power loss, equipment failure, or cyber attack, all dependent communications can fail simultaneously. This represents exactly the kind of cascading failure that emergency systems should avoid.

What Infrastructure-First Solutions Do Differently

Network-independent systems can use dedicated wireless infrastructure that operate independently of Wi-Fi and building networks. This infrastructure involves long-range, low-power radio protocols. Emergency signals don't need to compete with routine traffic. They travel on a separate pathway.

Punch Rescue's architecture uses distributed in-building devices to support coverage and location awareness. It can be designed so emergency reporting does not rely on Wi-Fi, even when Wi-Fi may be used when available for other functions.

Cellular Network Congestion

Relying on personal cell phones for emergency communication assumes that cellular networks will function during a crisis. Historical evidence suggests caution.

The Congestion Problem

During major incidents and mass gatherings, cellular networks have documented severe degradation. Voice calls may fail, messages may be delayed, and service may become unpredictable. This is partly because carriers design for typical peak loads, rather than extreme emergency surges.

Text messaging can be more resilient than voice calls in some surge conditions, but it is not guaranteed. FirstNet—a dedicated network for first responders—exists in part because consumer networks can become unreliable during emergencies.

What Infrastructure-First Solutions Do Differently

While internal communication within a building can use dedicated radio networks, communication to 911, to law enforcement, and to off-site administrators requires connectivity to the outside world. Infrastructure-first solutions often address this by adding dedicated external reporting pathways and designing for redundancy where feasible.

Punch Rescue's Base Station uses multiple redundant pathways to make sure emergency alerts reach responders and off-site administrators. The primary channel is wired Power over Ethernet (PoE), providing reliable connectivity through the building's network infrastructure. As backup, the Rescue Base Station includes multi-band cellular capability that continuously monitors all major carrier networks, automatically selecting the strongest available signal. Additionally, Rescue Repeaters include Wi-Fi capability, creating multiple potential pathways to the cloud for 911 and off-site notifications. This layered approach means the system attempts all available methods of internet access. Emergency signals can reach their destination even when individual pathways are compromised.

Cloud and Push Notification Dependency

Many schools use smartphone panic button apps that send alerts via cloud services. While convenient, these solutions depend on consumer notification infrastructure that is explicitly described as *best-effort* without guaranteed delivery or timing.

The Delivery Problem

Platform documentation and independent analysis indicate that push notification delivery can be variable and influenced by device state (locked/sleep), network conditions, user settings, and operating system power management. In short, push notifications are useful. They are not engineered though as a life-safety guarantee.

If a staff member's phone is on Do Not Disturb, has poor signal, or has a dead battery, a push alert may never arrive. If the local internet connection is slow, alerts may be delayed. In many cases, administrators cannot reliably confirm who received what in real time.

What Infrastructure-First Solutions Do Differently

Infrastructure-first approaches treat mobile-app alerts as one layer in a multi-layered system, rather than the sole channel. Hardware panic devices that use direct radio frequency transmission provide a redundant path that does not depend on smartphones, cloud servers, or notification settings.

Punch Rescue's system is designed so staff do not need to unlock phones, find apps, or navigate interfaces to initiate emergency reporting. The activation device can be worn on the person and designed for one-button activation.

Understanding "Degraded Conditions"

In technical discussions, "degraded connectivity" can sound abstract. In practice, it means:

- Partial delivery: Some people receive alerts; others do not. It may be hard to know who received what in the moment.
- Delayed delivery: Alerts arrive late, or are completely hindered until conditions improve.
- Unpredictable behavior: Systems work for some people, some of the time, without a clear pattern.
- Complete blocking: Congestion can produce queuing delays, dropped connections, and total failure.

A system that functions perfectly during normal conditions but fails during degraded conditions is not a reliable emergency system. It is a system optimized exclusively for common or ideal conditions.

Solution Categories: Perfect vs. Degraded Conditions

The critical evaluation question for any safety technology is: "What happens when power fails, networks congest, or everyone is on their phone?" If the answer is "the system won't work," that system may be insufficient for life safety.

A Performance Comparison

Solution Type	Ideal Conditions	Degraded Conditions
Smartphone Panic Apps	• Fast push notification delivery • Easy deployment, no hardware costs • Familiar interface for users	• Requires charged phone, unlocked screen, app open • Push notifications are "best effort" - no guaranteed delivery • Fails during Wi-Fi outages or cellular congestion • Cannot reach visitors, substitutes, non-enrolled users
Wi-Fi Dependent Systems	• Reliable when network operational • Integrates with existing infrastructure • Centralized management	• Complete failure if power affects access points • Coverage gaps in basements, stairwells, portables • Network congestion delays or blocks critical alerts • Single point of failure at network core
Two-Way Radio Systems	• Effective for routine communication • Familiar to emergency responders • Direct person-to-person contact	• "Throttling" during high-demand (documented at Parkland) • Building materials block signals (documented at Uvalde) • Limited cross-agency interoperability • Capacity limits when many users transmit
Hardware-Integrated, Network-Independent	• Reliable alert delivery and tracking • Building-wide coverage • Real-time location awareness • Simple one-button activation	• Battery backup maintains operation during power loss • Dedicated radio protocol bypasses network congestion • Mesh network provides redundant pathways • Simple activation works under extreme stress • Alerts all occupants, not just enrolled users

The Science of Simplicity Under Stress

In an emergency, human psychology becomes a decisive factor in whether a safety system succeeds or fails. This section translates key principles from psychology and human-factors engineering into practical guidance for evaluating emergency communication systems.

Simplicity under stress is more than a design preference. It serves as a functional requirement grounded in human physiology.

The Yerkes-Dodson Law: Why Stress Degrades Performance

Over a century ago, psychologists Yerkes and Dodson described an inverted-U relationship between stress (arousal) and performance. At low arousal (a.k.a. *boredom*), performance is suboptimal. Performance peaks at moderate stress. Beyond that peak, excessive stress causes performance to decline sharply.

In school emergencies, most people will be far past that optimal peak. Their cognitive and motor performance will be significantly impaired. This is not necessarily because they lack training or motivation, but because human physiology responds to threats in predictable ways.

Physiological Stress Responses

When adrenaline surges, the body prioritizes immediate survival over complex cognition. Research from law enforcement, military, and emergency medicine contexts documents consistent patterns:

- Many people under acute stress experience tunnel vision. Their peripheral vision narrows significantly.
- Many experience auditory exclusion. They may not hear alarms or verbal instructions clearly.
- People often act with reduced deliberation, relying on instinct and habit.
- Under high stress, fine motor control and complex cognitive tasks can degrade.

In practical terms, a teacher in fear for their life will rarely navigate a phone menu, type a code, or follow a multi-step procedure with calmness. They may fumble with keys, forget practiced steps, or freeze entirely. This is not a failure of character. It is human physiology under threat.

Procedural vs. Declarative Memory

Under extreme stress, the brain shifts from declarative memory (conscious recall of facts and instructions) to procedural memory (automatic, practiced actions). Neuroscience research shows that stress hormones contribute to this shift. People stop trying to logically remember what to do and instead fall back on habits and muscle memory.

This finding has profound implications for emergency system design. Under intense pressure, people tend to perform to the level of their training and repetition.

If a school's emergency plan requires on-the-spot complex decision-making, it will likely fail. Plans should leverage simple, well-practiced actions. This is the time to press one button, follow one route, or execute one procedure that has been drilled repeatedly.

Design Implications: The One-Button Concept

Any emergency device or interface should be as close to foolproof as possible. Under stress, cognitive capacity is severely limited. This is true for everyone, regardless of training or experience.

This is why infrastructure-first systems often use single-button wearable devices. When frightened, a teacher can press and hold one button to call for help. There's no unlocking a phone, finding an app, or entering a code. The simpler and more physical the action, the more likely it will succeed.

NASA human-factors guidance for emergency checklists emphasizes that they "must be easy to access, easy to read, and easy to use." This is because they must accommodate performance limitations under stress. Simplicity and clarity are necessary criteria for systems that must function during panic.

The Role of Drills and Familiarity

Because stress shifts memory processing to procedural memory, regular drills are essential for both compliance and for building the automatic responses that remain accessible under stress.

Many high-stakes operational environments emphasize repetition beyond initial competence specifically because deeply practiced procedures become more stress-resistant. For schools, this means that emergency systems should be used regularly for drills, for testing, and for routine operations.

This is why infrastructure that supports everyday use has a significant advantage. When staff use the same tools for daily coordination, check-ins, and routine communication, those tools become familiar. Familiarity creates procedural memory. Procedural memory survives stress.

Punch Rescue’s system is designed with this in mind. Self-testing supports routine verification. The dashboard supports daily visibility into system status. The same tools used for drills are the tools used in emergencies, building familiarity that can translate to reliability under pressure.

Summary: Design Requirements from Human Factors

Systems that require multi-step processes, app navigation, or complex decision-making are likely to fail when needed most. Simplicity is more than an aesthetic choice. It is a functional requirement grounded in human physiology.

The Regulatory Landscape

"Alyssa's Law" legal regulations, named in memory of Alyssa Alhadeff (who was killed at Parkland), increasingly require silent panic alarm systems in schools. Multiple states have enacted some form of this legislation, and additional states continue to consider similar requirements.

There is a growing recognition that emergency infrastructure requires a more dedicated investment.

State-by-State Overview:

State	**Year**	**Key Requirements**
New Jersey	2019	Silent panic alarm linked to law enforcement
Florida	2020	Mobile panic alert with real-time coordination
Texas	2023	Silent panic in every classroom; $17.1M in grants
Georgia	2025	Panic buttons in all schools; $108.9M in funding
Utah	2024	Wearable panic buttons; statewide RFP standards
New York	2023	Silent panic alarm systems
Tennessee	2024	Panic alarm systems in schools
Oklahoma	2024	Silent panic alarm requirements
Washington	2024	Emergency alert systems

Oregon	2024	Panic alarm legislation
Connecticut	2024	School safety alarm systems

*Additional states considering similar legislation: Multiple states have active proposals under review.

Common Compliance Requirements

While specific requirements vary by state, most Alyssa's Law legislation includes these common elements:

- Silent activation: Alarms must not alert an intruder to their activation.
- Direct law enforcement connection: Systems must alert police directly, while also communicating with school administrators.
- Real-time coordination: Responders should receive location information and be able to coordinate in real time.
- Building-wide coverage: Systems must cover the main offices, as well as *all* school buildings.

How Punch Rescue Addresses Compliance

Punch Rescue is designed to support the core requirements commonly found in Alyssa's Law statutes. This includes silent activation, direct law enforcement notification, and building-wide coverage. Specific compliance requirements vary by state and should be evaluated against the statute applicable to your jurisdiction.

Specific compliance-related features may include (depending on configuration and implementation):

- Silent panic activation with escalation pathways designed for rapid response
- Options for communicating incident location data to responders
- Data security and privacy controls appropriate for school environments
- Compatibility considerations for PSAP workflows (where applicable)
- Accessibility workstreams and compliance roadmap (where applicable)

Evaluating Emergency Communication Solutions

Given the documented challenges, technical dependencies, and human factors constraints described in this whitepaper, how should organizations evaluate emergency communication solutions? The following framework focuses on infrastructure resilience rather than feature counts.

These questions apply to any vendor, including us. We encourage you to ask them of every solution you evaluate.

Five Critical Questions

1. What happens when the network fails?

Every emergency communication system depends on some form of connectivity. The question is, what *kind* of connectivity? And what happens when it degrades?

- Does the system require Wi-Fi, cellular, or both?
- What happens if Wi-Fi access points lose power?
- What happens if cellular networks are congested?
- Does the system use an independent communication pathway (dedicated radio, mesh network) as backup?

2. What happens when the power fails?

Whether from weather, accidents, or deliberate action, power outages are common during emergencies.

- Do panic devices have on-board battery backup?
- How long can network infrastructure operate without building power?
- Are there single points of failure where one power loss eliminates communication?

3. Does the system work for everyone in the building?

Smartphone-based solutions only reach enrolled users with charged devices and enabled notifications.

- What about visitors, contractors, substitutes, or students who left phones in lockers?
- Does the system include building-wide alerting (strobes, sirens) independent of personal devices?
- What is the actual adoption rate of app-based components?

4. How simple is activation under stress?

Human factors research shows that complex interfaces fail under stress.

- How many steps are required to activate an alert? Can it be done with one action?
- Does activation require unlocking a phone, finding an app, entering a code?
- Is the activation device always on the person (wearable) or must they retrieve it?
- Is the system used regularly (drills, daily operations) to build procedural memory?

5. What documentation does the system provide?

When incidents occur, organizations must demonstrate due diligence. This requires documentation.

- Does the system log drill participation and completion?
- Does it provide testing records and device status history?
- Can you demonstrate that devices were functional at time of incident?
- Does the system provide evidence for compliance audits?

Infrastructure-First in Practice

What does infrastructure-first emergency communication look like when deployed? This section describes the key components and principles that define this approach.

Characteristics of Infrastructure-First Solutions

Based on the evidence presented in this whitepaper, infrastructure-first solutions share several defining characteristics:

Network Independence

They use private networks with mesh radio, LoRa, or similar protocols. These do not rely exclusively on congested public infrastructure. Emergency signals travel on dedicated pathways designed to continue functioning when Wi-Fi and cellular are impaired.

Power Resilience

They include battery backup in the data centers, in the devices and throughout the whole infrastructure. Wearable panic devices can operate independently of building power. Base stations and repeaters can include backup power designed for continued operation during outages.

Building-Wide Reach

They alert everyone in a building, including visitors, contractors, students without phones and enrolled app users. This can entail visual alerts (strobes), audio alerts (tones or announcements), and integration with existing PA systems.

Physical Simplicity

They provide wearable devices with one-button activation, accessible without unlocking a phone. Activation should be possible even when cognitive capacity is impaired by stress.

Location Precision

They offer room-level accuracy via dedicated infrastructure. They do not depend solely on GPS, which can be less precise indoors.

True Redundancy

They have multiple independent pathways at every layer, such as physical infrastructure, network connectivity, power supply, and human operations. No single point of failure should disable the entire system.

Why This Approach Matters

Many organizations are increasingly favoring hardware-integrated approaches. People want infrastructure resilience rather than software-only delivery.

Software is still essential for coordination, visualization, and management. Nevertheless, it may not address the infrastructure vulnerabilities documented in this paper. Hardware plus software, working together as an integrated system, can provide what neither can provide alone.

The Rescue Emergency Management System

Rescue hardware was designed to address the challenges discussed in this whitepaper. This section provides an overview of our platform and how it implements infrastructure-first principles.

No system can completely eliminate risk or guarantee outcomes during chaotic events. The goal is to reduce known failure modes wherever possible, and to support organizations in building more reliable, testable, defensible readiness.

We built the Punch Rescue ecosystem based on feedback we have received from safety and operations leaders who described recurring challenges. They were used to seeing coverage gaps, maintenance burdens, complex setup processes, false alarms, and limited testing workflows. Our goal was to build infrastructure that is simple to operate, designed for reliability, and built to support ongoing preparedness.

The Punch Rescue Ecosystem

Rescue Cards: Wearable Panic Buttons

Rescue Cards are wearable panic devices designed for simple emergency activation. Features may include:

- Multiple reporting modes (e.g., testing and tiered alerting), depending on configuration
- Long-life battery design with replaceable batteries
- Visual confirmation via device indicators
- Lightweight wear options (lanyard, belt clip)
- Does not require Wi-Fi for emergency reporting, even though Wi-Fi may be used when available for other functions

The Rescue Card embodies the human factors principles discussed earlier. It has one-button activation, it stays continuously present on the person, and it is designed to be operable under extreme stress.

Rescue Repeaters: Coverage and Location Tracking (Patent Pending)

Rescue Repeaters are in-building devices placed strategically throughout a facility. They can support:

- Room-level location awareness
- Signal rebroadcasting to reduce coverage gaps

- Local processing to keep emergency signals fast and reliable
- Optional visual alert components (e.g., strobes), depending on installation
- Mesh routing so signals can find alternate paths if one route is blocked

Repeaters work together to support building-wide coverage. Unlike systems that depend on Wi-Fi, the mesh network is designed so emergency reporting can remain functional even if building internet is unavailable.

Rescue Base Stations: Central Hubs with Cellular Capability

Each site is provided with a Rescue Base Station that serves as a central hub for the system:

- Receives emergency signals from Rescue Cards and Rescue Repeaters
- Includes a cellular pathway intended for external emergency reporting
- Supports audible and visual building alerting options, depending on configuration
- Provides local controls for testing and alert management

The Rescue Dashboard: Monitoring and Real-Time Visibility

The Rescue Dashboard supports system visibility and monitoring, which may include:

- Overview of devices and status
- Location visibility on maps (depending on mapping scope and setup)
- Alerts for offline devices, battery status, and emergency events
- Reporting outputs that support testing and documentation

Integration Capabilities

Punch Rescue can integrate with third-party platforms to support messaging and workflow coordination, depending on customer needs and implementation scope.

What Makes Punch Rescue Different

We designed the Rescue devices based on direct feedback from administrators and safety leaders and focused on a few priorities:

Effortless Setup

Rescue devices are designed to be straightforward to deploy. Systems can be provided pre-configured, with guided setup and optional implementation support.

Real-Time Awareness

With in-building repeaters and mapping, the system can provide near real-time location awareness to support faster, clearer response.

Low Maintenance

The platform is designed to minimize maintenance burden through long-life batteries, proactive monitoring, and remote software update workflows.

Reliable Coverage (Patent Pending)

Rescue Repeaters are designed to support building-wide coverage and reduce dead zones. Emergency reporting is designed not to rely on Wi-Fi, while still using Wi-Fi when available for non-critical functions.

Implementation Considerations

Deploying emergency communication infrastructure is clearly an IT decision, but it's also an organizational commitment. This section provides practical guidance for proper implementation.

Pilot Programs: Start Small, Learn Fast

For organizations evaluating new emergency communication systems, pilot programs offer a low-risk way to test performance in real-world conditions before district-wide deployment.

Benefits of piloting:

- Validate performance claims in your actual building environment
- Identify coverage gaps or dead zones specific to your facilities
- Train staff and build familiarity before high-stakes deployment
- Gather internal champions who can advocate based on direct experience
- Reduce political friction by demonstrating value before requesting full budget

Punch Rescue offers pilot programs that allow districts to evaluate the platform in a limited scope, such as within administrative buildings, individual schools, or specific wings. This program runs before committing to a broader deployment, and it lets the technology’s performance speak for itself.

Training and Adoption

As discussed in the human factors section, familiarity is critical. A system that staff don't know how to use regularly will likely fail under stress.

Recommendations:

- Conduct regular drills that exercise the actual emergency communication system
- Enable easy self-testing so staff can verify their devices work
- Integrate emergency tools into daily operations where appropriate
- Provide refresher training, especially for new staff and substitutes

Punch Rescue includes onboarding and training options because we know implementation is not complete until staff are confident using the system.

Integration with Existing Systems

Most schools have existing emergency infrastructure with PA systems, notification platforms, and security cameras. New emergency communication systems should complement existing investments, not require a complete replacement.

Questions to consider:

- How does the new system integrate with existing PA or intercom systems?
- Can it work alongside existing notification platforms (for redundancy)?
- What data sharing is possible with security and first responder systems?
- Does integration require significant IT resources?

Ongoing Maintenance and Support

Emergency infrastructure requires ongoing attention. Devices need battery replacement, software needs updates, and systems need testing.

Punch Rescue's approach is designed to minimize the maintenance burden through:

- Over-the-air software update workflows
- Proactive monitoring and alerting
- Battery replacement and device lifecycle processes appropriate for long-term deployments

The Bottom Line: Making Defensible Decisions

This whitepaper has examined emergency communication through the lens of *infrastructure resilience.* We want to see an impressive performance under degraded conditions.

What the Evidence Shows

Real emergencies can create cascading infrastructure challenges. Official investigations from Parkland, Uvalde, Virginia Tech, and other incidents have documented how networks congest, power fails, and systems designed for normal conditions may break down.

Software-only solutions have inherent limitations. Push notifications are best-effort, Wi-Fi requires power, and cellular networks can degrade during extreme surge conditions. These are documented realities from major incidents.

Human factors matter. Under stress, cognitive capacity shrinks, fine motor skills deteriorate, and people revert to trained habits. Complex interfaces fail precisely when they matter most.

Regulatory momentum is building. The spread of “Alyssa's Law” legislation indicates there is a growing awareness in society that emergency infrastructure requires a more dedicated investment.

The Defensibility Standard

When evaluating emergency communication solutions, *defensibility* is the one criterion that should take precedence. Can you demonstrate to your board, to regulators, to the media, and in litigation that you made a reasonable, well-informed decision?

This standard requires:

- Understanding the actual failure modes of your current system
- Evaluating solutions based on *infrastructure resilience* rather than feature comparisons
- Documenting your decision-making process and the evidence you considered
- Implementing regular testing, drills, and training to build procedural memory that survives stress

No system can guarantee outcomes in chaotic, violent situations. But we can all reach for a more reasonable, documented preparation that demonstrates an authentic organizational commitment to safety.

Next Steps

If the principles in this whitepaper resonate with your approach to school safety, we invite you to learn more about how Punch Rescue implements them in practice.

Schedule a Demo: See Punch Rescue's platform in action and understand how it addresses the challenges at hand.

Explore a Pilot Program: Test Punch Rescue in your environment before committing to a district-wide deployment. *Reach out to our partner and sales team at sales@punchrescue.com to inquire about available pilot program openings.*

Register for a Webinar: Join a live session to ask questions and see demonstrations. Visit our website to learn more about upcoming webinars, trade shows and demonstrations.

Appendix: Sources and References

Official Reports and Commission Findings

- Marjory Stoneman Douglas High School Public Safety Commission Reports (2019-2024)
- U.S. Department of Justice Critical Incident Review: Robb Elementary School, Uvalde, Texas (January 2024)
- Virginia Tech Review Panel Report to Governor Kaine (August 2007)
- Uvalde's Critical Incident Review (February 2024)

News Coverage and Documented Sources

- ABC News, NBC News, CNN coverage of Apalachee High School incident (September 2024)
- Georgia Recorder coverage of Georgia Alyssa's Law passage (March 2025)
- Sun-Sentinel reporting on Parkland commission testimony

Emergency Response Research

- Post-incident reports and after-action analyses from major school emergency responses
- FCC and telecommunications industry documentation on network congestion during mass events
- FirstNet Authority resources on public safety communication requirements

Technical Documentation

- Apple Developer Documentation: Push Notification Best Practices
- FCC: Wireless Emergency Alerts Technical Requirements
- LoRa Alliance: Long Range Wide Area Network specifications

Human Factors Research

- Yerkes, R.M. & Dodson, J.D. (1908): The Relation of Strength of Stimulus to Rapidity of Habit-Formation
- NASA Human Factors Guidelines: Emergency Procedures Design
- FAA Human Factors: Checklist Design Principles
- Stress response research and human performance literature relevant to emergency contexts

Regulatory Sources

- State legislation: NJ A764; FL SB 70; NY S7132A; TX SB 838; TN HB 322; UT HB 84; OK SB 1357; GA SB 17; WA SB 5004; OR HB 3101; CT SB 1216
- Utah statewide RFP requirements for school safety systems
- Clery Act: 20 U.S.C. § 1092(f)