

Workforce Technology Solutions Playbook Series: Workplace Violence Prevention

Solution Purpose: Prevent and actively respond to workplace violence

A variety of technology solutions exist to support organizations in reducing and responding to workplace violence. For the most comprehensive approach, it is recommended that organizations begin with an Enterprise Security Risk Management (ESRM) assessment. An ESRM assessment provides a holistic understanding of risk across the organization and informs continuous improvement efforts related to systems, partnerships, strategic alignment, and overall risk mitigation. [Convergent](#) is a Minnesota-based solution provider that performs healthcare ESRM assessments (contact [Eric Hinz](#) for additional information).

This playbook specifically focuses on the adoption of mass communication and rapid-response systems, which represent one critical component of managing and responding to workplace violence and other critical incidents. The platforms included offer a range of capabilities, such as:

- Real-time alerts and mass communication, including panic buttons
- Visitor management and entrance control
- Incident reporting and management
- Data analytics and dashboarding
- Training and awareness management

How These Technologies Work:

Mass communication and rapid-response systems support organizations in preventing and responding to workplace violence and other critical incidents. While each platform differs, most systems function through a combination of alerting tools, communication networks, data capture, and workflow automation. Below is a simple overview of how each core capability works.

Workforce Technology Solutions Playbook Series: Workplace Violence Prevention

1. Real-Time Alerts & Mass Communication (Including Panic Buttons)

- Staff use wearable or mobile panic buttons to instantly signal an emergency.
- The system identifies the staff member's location using Wi-Fi, Bluetooth beacons, LoRaWAN, or GPS.
- Alerts are immediately sent via text, push notifications, desktop pop-ups, overhead paging, or digital signage.
- Enables fast, coordinated responses across the organization.

2. Visitor Management & Entrance Control

- Visitors check in through kiosks or digital systems that issue badges or time-limited credentials.
- Staff receive notifications when visitors arrive, and systems can flag restricted or high-risk individuals.
- Integrates with door access systems to manage entry, lock/unlock areas, or alert staff to forced-entry events.
- Improves visibility and control over who enters the community.

3. Incident Reporting & Management

- Staff can quickly submit incident reports through mobile or desktop tools.
- Systems route reports automatically to HR, administration, or security.
- Data is stored in a centralized log to track violence, threats, near misses, or unsafe behaviors.
- Supports consistent documentation and regulatory requirements (e.g., OSHA, CMS).

4. Data Analytics & Dashboards

- Systems collect information from alerts, visitor logs, incident reports, and response times.
- Dashboards display trends, hot spots, and response performance.
- Organizations can identify patterns (e.g., high-risk units or times of day) and adjust staffing or interventions.
- Some platforms offer predictive analytics to anticipate emerging risks.

5. Training & Awareness Management

- Platforms often include built-in training modules for system use, safety procedures, and de-escalation skills.
- Automated reminders track training completion and support compliance.
- Some tools support drills and simulations, helping teams practice emergency scenarios.
- Reinforces preparedness and builds a strong safety culture.

Budget:

Budget requirements vary significantly depending on scope, features, scale, and integration needs. Some vendors offer standalone pricing for mass communication and panic button systems, while enterprise-level platforms—with a broader suite of services—are priced separately.

Pricing structures also vary across providers. Examples include:

- **Per-user pricing:** Typically ranges from \$1.50 to \$20 per user, depending on feature sets, scale, and contract terms.
- **Square-footage pricing:** Some tools price by facility size, with individual components ranging from \$1,000 to \$8,000 per year. Mass communication and panic button capabilities are usually core services and fall on the higher end of this range.
- **One-time installation and implementation costs:** Often billed separately and can range from \$200 to \$5,000 per service or site, depending on the complexity of the system being deployed.

This range of pricing allows organizations to tailor solutions based on their needs, available resources, and desired level of integration.

Specific pricing for each vendor is not included in this playbook because the fees structures vary and can change over time. Contact information for each solution is included in the matrix to access accurate pricing.

VENDOR MATRIX

CENTEGIX (CRISIS ALERT)

SINGLEWIRE (INFORMACAST)

ALERT MEDIA

FEATURES

INITIAL TRAINING INCLUDED IN SET UP COST?



ADDITIONAL TRAINING OFFERED FOR ADDITIONAL COST?



ACTIVE PRESENCE IN MN?



WORKS ON DESKTOP?



WORKS THROUGH MOBILE APP?



OFFERS CENTRALIZED MONITORING SYSTEM?



OFFERS VISITOR MANAGEMENT



OFFERS REAL-TIME TRACKING

Employees

Employees, Residents, Visitors

Employees, Residents

CAPABLE OF DIRECT 911 CALLS



INFRASTRUCTURE NEEDS

- Operates on an independent LoRaWAN/Bluetooth network.
- Requires facility-placed beacons and gateways to enable full indoor/outdoor coverage.
- Does **not** rely on Wi-Fi or cellular networks.
- Provides reliable, real-time alerting and location tracking without adding load to existing IT systems.

- Supports both **hybrid cloud** and **full cloud** architectures.
- Hybrid Model:**
 - Integrates with on-premises systems (IP phones, overhead paging, digital signage, physical security systems).
 - Requires an on-premises server hosted on VMware or a hardware appliance.
- Full Cloud Model:**
 - Supports mobile devices, desktops, and Microsoft Teams.
 - Fully cloud-hosted with no customer infrastructure required.

- Fully web-based platform accessible via any modern browser.
- Requires reliable, high-quality internet connectivity.
- Depends on appropriate network redundancy to maintain consistent availability.

VENDOR MATRIX

CENTEGIX (CRISIS ALERT)

SINGLEWIRE (INFORMACAST)

ALERT MEDIA

FEATURES

TOP INTEGRATIONS

- Phone systems
- Digital signage
- Nurse call
- E911
- Visitor Management
- Security Systems
- Access Control

- Phone systems
- Digital signage
- Nurse call
- E911 Systems
- Visitor Management
- Case Management
- Security systems/Cameras
- Access Control
- Resident wander systems

- Phone systems
- Digital signage
- Nurse call
- E911 Systems
- Visitor Management
- Case management
- Security systems/Cameras
- Access Control

CONTACT

Kyle Herndon
614-209-3825
kherndon@centegix.com

Dave Nelson
608-421-7288
Dave.nelson@singlewire.com

Zach Balod
817-681-4043
Zach.balod@alertmedia.com

WEBSITE

www.Centegix.com

www.Singlewire.com

www.AlertMedia.com

IMPLEMENTATION

Key Personnel for Successful Implementation

Project Lead(s): (responsible for internal coordination and vendor communication):

- Personnel to consider for Project Lead role: Security team, Administrator or Assistant Administrator, Human Resources

Notes:

- Use co-leads to ensure continuity during turnover, illness, or leave.
- If you have a union, inform the union representative of plans to deploy mass communication or alerting technology.

End-users: (Individuals and groups who will interact with the software and hardware)

- Administration
- Human Resources
- Security
- All employees
- Depending on the solution and features: residents, visitors, volunteers

Vendor Selection Team: (Stakeholders with decision-making authority or subject-matter expertise)

- Project Lead
- Administration
- Human Resources
- Front desk/visitor management
- IT/Tech support
- Security
- Plant maintenance
- End-user representative(s)

Team/Staff to Support Product Launch: (Key roles for training, troubleshooting, and promoting adoption)

- Project Lead
- Human Resources
- Staff education/training
- IT/Technical support
- Security
- Plant maintenance
- End-user representative(s)

Follow-up Supporting Coalition Team: (Individuals who play a key role with reinforcing the rollout success because of their job description and/or leadership responsibilities)

- Project Lead
- Human Resources
- Operations/Administration/Executive Director

IMPLEMENTATION

Best-Practice Implementation

Key Software Integration/Compatibility:

- Solutions often integrate with nurse call systems, physical security systems, Microsoft Teams, and door-access technology. The depth of integration depends on selected services and vendor capabilities.
- Most platforms use some form of real-time locating services (RTLS).
 - * Location tracking may activate only when a panic button is pressed or may operate continuously.
 - * RTLS can be triggered via wearable devices or mobile phones.
 - * Clarify RTLS capabilities and privacy protections during vendor discussions.

Infrastructure/Equipment Requirements:

- Most systems are web-based and accessible via computer, tablet, or mobile device.
- Redundancy is important for power and internet outages.
- Wireless communication requirements vary:
 - * Some platforms rely on Wi-Fi.
 - * Some platforms use independent networks (e.g., Bluetooth beacons, LoRaWAN).

Expected Implementation Timelines after Vendor is Selected:

- **4 weeks** if selecting a basic panic button system
- **6-8 weeks** if selecting more features or integrations

Policies & Procedures to Review/Update:

- For unionized environments, ensure policy changes align with union contract requirements, including any necessary notification or negotiation.
- All emergency preparedness related policies/procedures should be reviewed and updated to account for the mass communication tools and notification processes.

What to Expect Post-Implementation:

- With improved tools for communication and response, emergency drill compliance should improve, building confidence in overall safety culture.
- Successful implementation will be reflected by this system being embedded in the culture and communication work-flows.

IMPLEMENTATION

Key Considerations & Tips:

- **Union considerations:** Communicate early, follow contractual requirements.
- **RTLS considerations:** Clarify privacy, activation triggers, and data use.
- **Connectivity considerations:** Plan for redundancy and network reliability.
- **Features vs. cost:** Align technology choices with organizational goals and safety impact.
- **Integrations:** Identify which existing systems must connect to the new solution.
- **Stakeholder communication:**
 - Develop a communication plan for staff, residents, families, visitors, and vendors.
 - Educate stakeholders on changes to entry processes and emergency response expectations.
 - Clear communication strengthens trust, confidence, and preparedness.

What's Next for This Technology?

Advancements in artificial intelligence and integrated security systems will significantly expand capabilities in workplace violence prevention.

Ask your solution provider about progress in the following areas:

- **Artificial Intelligence & Predictive Analytics:**
Automated analysis of video, access-control logs, and communications to identify patterns of risk; computer vision for unusual behavior; natural language processing to detect threatening communications.
- **Integrated, Centralized Security Systems:**
Unified platforms connecting video surveillance, access control, mobile alerts, incident tracking, and analytics to shift from reactive to proactive safety management.
- **Near-Miss & Pre-Event Data Capture:**
AI-enabled tools that identify precursor behaviors—such as aggressive interactions or unauthorized presence—to support early intervention and predictive modeling.

Playbook Development and Disclaimer:

This playbook was developed to assist providers in understanding workplace violence prevention technologies; it does not capture all available systems. Included products were selected based on the following:

- Recommendations from LeadingAge Minnesota members
- Information from solution providers
- Product demonstrations and Q&A sessions
- Feedback from active users
- Provider case studies

Use this playbook as a general guide to understand solution functionality and support successful implementation. Solutions referenced have **not** been tested or verified by LeadingAge Minnesota. Providers should conduct their own due diligence—including demonstrations, reference checks, and site visits—prior to final vendor selection.