Critical Manufacturing Sector Active Assailant Post-Incident Best Practices Guide

March 2024

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Contents

Overview

The Critical Manufacturing (CM) Sector Active Assailant Post-Incident Best Practices Guide serves as a resource for post-incident response and recovery efforts for the CM Sector and its partners. Planning, preparing, and implementing essential response and recovery processes are crucial steps. They help all critical manufacturing organizations and affiliates to remain resilient in the face of any active assailant incident.

An **active assailant** is an individual actively engaged in killing or attempting to kill people in a confined and populated area.[1] These assailants may attack using firearms, vehicle-ramming tactics, bombs, incendiary devices, chemical weapons, drones, or other methods. After an organization experiences an active assailant incident, it must take two equally important steps. The first is **immediate response**—the initial actions taken by personnel after an incident to save lives and minimize damage. After these measures are taken, the next step, **recovery**, begins, both **short-term recovery**—re-establishing safety and mitigating the physical, psychological, and emotional impacts in the days, weeks, and months following the incident; and **long-term recovery**—helping the organization resume operations and helping those impacted return to a sense of normalcy in their daily interactions and professional life, a process that will likely take years. Be aware that there is no sharp distinction between these steps: immediate response will blend into the days following an incident, just as short-term recovery will extend into the subsequent months.

The measures outlined in this Guide may vary dramatically by type of organization (e.g., an office vs. a factory, a single company building vs. an organization spread across multiple locations, or a large company with significant resources vs. a small company with limited personnel). The size of an organization in particular impacts response and recovery efforts after an incident. For instance, small and mid-size companies may require their leadership team and a limited number of employees to assume multiple roles and responsibilities that a larger organization might distribute more broadly across its workforce. Small and mid-size companies also lack the resources of a larger organization and may wish to, or need to, outsource some of the services mentioned in this Guide rather than relying on in-house measures and personnel, from information technology (IT) services to legal responsibilities. To best prepare for an incident and ensure worker safety and business continuity, an organization must take available resources, employees, building(s), and the nature of their operation into account.

Most of all, a critical manufacturing organization must make these preparations long before an active assailant incident takes place. Without proper planning, task delegation, community connections, and an understanding of the wide-reaching impact of an active assailant incident, successful response and recovery are unlikely.

Disclaimer

The Cybersecurity and Infrastructure Security Agency (CISA) does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Physical Security Performance Goals," accessed January 12, 2024, https://www.cisa.gov/resources-tools/resources/physical-security-performance-goals-faith-based-communities.

Part One: Immediate Response

The **immediate response** phase focuses primarily on an organization's immediate actions to save lives, reduce physical and mental health impacts, ensure public safety, and meet the needs of the people affected. Before beginning to think about properly recovering from an incident, a company must first know how to respond initially to the incident itself. Effective, efficient, and timely response relies on having risk-informed preparedness measures in place.

Owners and operators should educate as much of their staff as thoroughly as possible on basic life-saving procedures, such as first aid and CPR, that may be needed before emergency services arrive on the scene of an incident.[2] However, effectively navigating the complex and time-sensitive steps required for immediate response necessitates a more organized company-wide approach, which includes outlining and delegating the following responsibilities, starting at the top of the organization.

C-Suite Responsibilities

High-level leadership, often referred to as C-suite executives, plays a vital role in developing, committing to and engaging with their organization's incident response measures. In the face of an emergency, employees look to the organization's leaders for guidance. Executives should participate and play an active role in the exercising of any company plans, training courses, or safety measures. They should lead the charge on these efforts for the rest of their organization.

If executives are dismissive and uninformed about active assailant or other threats, their employees will be more likely to adopt the same mindset. Conversely, if employees observe that high-level leadership is committed to developing and implementing a thorough emergency action plan (EAP), they are more likely to take the threat seriously as well. If company leaders are panicked or indecisive in the face of an incident, their employees may react similarly. But if leadership is confident, decisive, compassionate, and informed during and after an incident, their employees are more likely to take their lead and conduct emergency response measures efficiently.

High-level leadership should actively participate in the planning and execution of these measures. This involvement can take various forms, such as leading or assigning regular training courses on emergency management and first aid or sharing incident response information in the form of fliers, posters, or other accessible guidelines within their facilities or offices.

Emergency Management Responsibilities

The most vital step an organization can take in carrying out a seamless, effective, and efficient immediate response is creating an EAP. This should be a whole-of-organization plan involving all employees (including C-suite executives, as noted above). When faced with an active assailant incident, all personnel should have an assigned role they are familiar with and confident in conducting to ensure they and the rest of their organization are safe. Depending on the size of the organization and its available resources, this plan will also involve external services such as outsourced IT, Human Resources (HR), and security personnel. Each organization must consider their unique situation when developing their immediate response plan.

Each role and responsibility included in the EAP should be clearly defined and delegated to specific individuals or teams among the organization's employees. Without clearly designated roles, many employees will be unlikely or unable to take proper action in the wake of an emergency. Consider employees' varying schedules, access to

---

[2] Stop The Bleed®, "Get Trained!", accessed July 12, 2023, https://www.stopthebleed.org/training/; Federal Emergency Management Agency (FEMA), "You Are the Help Until Help Arrives," accessed July 12, 2023, https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US.

different floors or areas of the facility, and proficiency in written and spoken English when assigning these roles. If applicable, involve the organization's labor union(s) early in the emergency planning process; they may be useful resources in determining facility-specific plans, assigning roles, and ensuring that any employee concerns are met.[3]

When creating its EAP, an organization's leaders, as well as its Security Director (or any equivalent role that will deal directly with law enforcement and first responders) should be trained in the National Incident Management System (NIMS).[4] Other federal tools to help organizations develop comprehensive and personalized violence response plans include the Office for Victims of Crime's toolkit,[5] the Federal Emergency Management Agency's (FEMA) preparedness guide,[6] and the Occupational Safety and Health Administration's (OSHA) EAP eTool.[7] An organization's leaders should be familiar with and well-versed in all of these resources. They should revisit these resources routinely (e.g., annually) to refresh their memories and ensure their information is up to date.

Immediately following an active assailant incident, the EAP should initiate the following procedures, which should be designated, developed, and exercised well in advance of an incident.

Notification System

Incident response in the wake of an active assailant incident should begin with notification. The EAP should establish a system to notify all staff on site of an incident, including when to advise them to evacuate or to shelter in place.[8] The person(s) responsible for triggering this notification system should be established in advance. The organization may include pre-scripted messages, which should be adaptable to the situation at hand.

If applicable, coordinate with the organization's union(s) to ensure that this notification system can be received and understood by all employees, including those with language barriers or access and functional needs, as well as those in loud, isolated, or closed-off areas of the facility. A notification must also be sent to employees who are not on site (e.g., workers who are at a different facility, not scheduled to work that day, or conducting any offsite work) advising them to avoid the facility due to an ongoing incident.

Evacuation Routes

An organization's leadership (e.g., floor managers, executives, or supervisors, depending on the building in question and employees' familiarity with its layout) should map out evacuation routes prior to an incident and ensure that all employees are familiar with them. Routes should be physically accessible for occupants with access and functional needs. This includes all potential visitors to the site, in addition to existing staff. The organization should post a map of these evacuation routes throughout its building(s) and keep a copy in the EAP, updating it as needed.

This plan should include at least two evacuation routes and be practiced routinely (e.g., annually) by employees to account for any blockages, hazards, cut-off pathways, or other barriers that may emerge during or immediately after an active assailant incident. Depending on the nature of the attack, already-practiced fire drill routes may not be safe or even possible to follow, so contingency routes should be predetermined. Nontraditional exits, like

---

[3] CISA ISC, *Violence in the Federal Workplace: A Guide for Prevention and Response,* 2019, https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide.
[4] FEMA, "National Incident Management System," accessed July 13, 2023, https://www.fema.gov/emergency-managers/nims.
[5] Office for Victims of Crime Training and Technical Assistance Center, "Mass Violence and Terrorism," accessed July 13, 2023, https://www.ovcttac.gov/massviolence/?nm=sfa&ns=mvt&nt=hvmv.
[6] FEMA, *Are You Ready?* updated April 2023, https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf.
[7] Occupational Safety and Health Administration (OSHA), "Emergency Action Plan," accessed July 13, 2023, https://www.osha.gov/etools/evacuation-plans-procedures/eap.
[8] Federal Emergency Management Agency (FEMA), *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101,* September 2021, https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf.

windows and rooftops, can be used as evacuation routes if needed. Ensure that employees have the means (e.g., keys, glass-breaking tools) to access them.

Critical manufacturing organizations' evacuation routes will depend on the building's location, layout, and the nature of the manufacturing operation. They must address a number of questions when planning evacuation routes, including:

- Are the employees in an office environment or on a manufacturing floor?
- Does the company have a single location or are employees spread across multiple buildings?
- Does the building have a security system that must be considered?
- Is there machinery that must be shut off prior to evacuation?
    - If machinery must be shut down or disabled prior to evacuation, ensure that employees (e.g., individual factory workers, floor managers, or other relevant personnel, depending on the organization's layout) are able to do so quickly, efficiently, and without fear of repercussions for interrupted operations. However, ensure that employees understand that their safety is the organization's top priority; if manufacturing equipment cannot be disabled in time, they should proceed to the evacuation route as quickly as possible.

If an organization is unsure of how to plan evacuation routes for their building, they can contact local law enforcement, who may be able to visit their facility and help plan the best routes.

In addition to establishing evacuation routes, ensure that employees know the following best practices for evacuation:

- Leave personal belongings behind.
- Raise your hands in the air to signal that you are unarmed to responding law enforcement.
- Avoid escalators and elevators.
- Take others with you, but do not stay behind because others refuse to leave.
- Call 9-1-1 as soon as it is safe to do so.

When calling 9-1-1, provide as much of the following information to dispatchers as possible:

- Location of incident, including street address, building number, floor, and any other necessary information (e.g., Room 123, Loading Bay 4);
- Location of caller;
- Location of active assailant (and the number, if more than one);
- If there is law enforcement or security personnel on site, if known;
- Physical description of attacker(s), if known;
- Type and number of weapons used by attacker(s), if known;
- Use or threat of explosives/improvised explosive devices (IEDs);
- If attack is still occurring; and
- Number of potential victims at the scene.

When evacuation is not possible due to the location of the assailant(s) or resulting damage, employees should be aware of secure shelter areas within the facility—these will ideally have a locking door and as much concealment and cover as possible. Employees sheltering in a secure area in the facility should remain in place until informed by responding emergency services that it is safe to move.

Accountability Groups

When evacuating, the most important goal is for employees to get out as quickly as possible. In practice, this

means that many people may leave the building(s) from multiple exits, making assembling after an evacuation and accounting for missing employees difficult. The EAP should designate certain personnel (e.g., floor/facility/area managers) to an accountability group to keep track of personnel following an evacuation. Accountability is the process through which an organization determines the status and location of its personnel; this process will also include assisting law enforcement and emergency medical services with recovery and facilitating eventual family notifications.

The EAP should inform all evacuees to seek safety in nearby indoor locations, if possible (e.g., offices, hotels, or conference centers), to accommodate unpredictable weather. It should also instruct employees to avoid lingering in company-adjacent parking areas, since attackers may have left IEDs in vehicles.

When possible, choose a location with enough space to accommodate all on-site personnel, as well as specific spaces (e.g., rooms, tents, or adjacent buildings) that the accountability group can designate for emergency services, police, media, families and loved ones, and those in need of medical care. In particular, the media and press should be directed to a specific, separate location to keep them away from impacted families and employees and out of the way of responding emergency services. The accountability group must also consider the potential requirements of all personnel once evacuated, including physical accessibility at their location(s) and access to resources in other languages.

The accountability group will take note of all personnel accounted for, missing, and injured, keeping their lists up to date as the situation unfolds. This group should be aware ahead of time of any employees working off-site or absent from the organization, as well as all personnel on site (e.g., employees, patrons, contractors, and vendors). However, simple headcounts may not be accurate or even possible; evacuees may be unable to gather in a single location, and some personnel may have been unable to evacuate and are still sheltering inside the building(s). For this reason, the EAP may consider the use of accountability tools such as an app check-in.

The group will also share this information with emergency services to facilitate medical aid and reunions with families and emergency contacts. Note that if minors are among the evacuees, organizers must take extreme care to properly identify their parents or guardians to ensure their welfare.

Taking these steps to predetermine an adequate accountability plan will encourage discussion while creating the EAP to identify and plan for associated response efforts, such as coordinating sufficient resources (e.g., food, drinks, therapists, clergy) that evacuees and responders may need.

Medical Operations Groups

The medical operations group consists of clearly designated personnel to address immediate needs and ensure physical safety after rescue (e.g., immediate first aid, CPR, delayed first aid, morgue). Some larger organizations may already have a medical operations group in place, though most small and mid-size companies will need to assign these roles to their employees as part of their emergency management plan.

Whenever possible, the medical operations group should include personnel who are trained in first aid and CPR. This may necessitate the organization to provide first aid training or require CPR certification for some or all of its employees. Existing resources can help organizations and their employees understand what they need to know and can teach them basic, accessible first aid, as well as when to use it and how to coordinate with responding emergency services groups; these resources include the American College of Surgeons' Stop The Bleed® initiative[9] and FEMA's You Are the Help Until Help Arrives.[10] Armed with these skills, the medical

[9] Stop The Bleed ®, "Get Trained!", accessed July 12, 2023, https://www.stopthebleed.org/training/.
[10] Federal Emergency Management Agency (FEMA), "You Are the Help Until Help Arrives," accessed July 12, 2023, https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US.

operations group's responsibilities include helping survivors and evacuees get to hospitals or other assembly/relocation areas and supporting all efforts to transport victims unable to be treated at the scene to medical facilities.

The medical operations group should be able to provide all emergency and medical personnel with any necessary information about the incident to assist in treatment. This effort requires knowledge of all nearby medical facilities and their capabilities/trauma levels.[11]

Be aware that comprehensive preparedness requires more than just awareness of the nearest hospital. Other facilities may be required depending on specialized care needs or other factors (e.g., road blockages following the incident that make a secondary location or backup plan necessary).

Depending on their resources, some larger organizations may have a Security Director or other designated official who already has knowledge of their area's medical facilities and their capabilities as well as established relationships with those facilities and with state/local law enforcement. An existing relationship with these facilities is critical for efficient communication during and after an active assailant incident. Organizations without a previously established Security Director must ensure that their medical operations group reaches out to these groups to develop basic familiarity and enable a positive and seamless working relationship in the event of an incident. A hospital can quickly become overcrowded after an incident if many people were wounded; the ability to communicate as early as possible with hospitals can help emergency services prepare and organize sufficient care for victims, though arrival to the hospital and distribution of care may still be a chaotic process.[12]

Utility Security Groups

Depending on the assailant's motives and methods, considerable damage may be done to an organization's cyber and physical assets, including manufacturing equipment, computers and online systems, security systems, and manufactured products. Utility security groups should be established to ensure the cyber and physical security of these assets and mitigate the risk of theft or compromised data in the wake of an incident.

Larger critical manufacturing organizations may have cyber and physical security personnel or offices that function as utility security groups. However, small and mid-size companies will likely need to establish their own. Depending on the organization's size, layout, and resources, its cyber and physical security may be managed by a third-party company (e.g., an offsite IT provider may provide cybersecurity services to the company). If so, these third parties should be alerted as soon as possible in the event of an active assailant incident and be kept up to date to prevent cybersecurity breaches or data theft. The organization should ensure a backup form of communication to reach this company in case of power outages or systems shutdowns (e.g., email, cell phones, landlines).

Specifically, utility security groups should be managed by the IT department (in-house or outsourced, depending on the organization's structure) and a physical security team, led by a Physical Security Director. This individual is the organization's lead on all physical security matters and, in collaboration with the IT department, provides unified security risk management support and leadership across the organization. While some critical manufacturing organizations have an established physical security team and Director in place, others—especially those with fewer resources, smaller facilities, or lower security levels, do not. These organizations will need to assign these responsibilities themselves, whether to existing employees (e.g., supervisors, floor managers, other responsible and knowledgeable personnel) or to the head of security for the organization's building, facility, or

[11] Health Resources and Services Administration, "Find a Health Center," accessed July 13, 2023, https://findahealthcenter.hrsa.gov/.
[12] Administration for Strategic Preparedness and Response (ASPR), Technical Resources, Assistance Center, and Information Exchange (TRACIE), "A Day Like No Other—Case Study of the Las Vegas Mass Shooting," 2018, https://asprtracie.hhs.gov/technical-resources/resource/6472/a-day-like-no-other-case-study-of-the-las-vegas-mass-shooting.

complex. IT and physical security personnel must have seamless communication with one another and with the rest of the organization.

Active assailant incidents are frightening and unexpected, and people often are reluctant to act in the face of a threat, especially if they are the first in their location to initiate emergency protocols. The more familiar an organization and its staff are with their emergency management plans, the more confident they will be in carrying them out and the more willing and able they will be to help other facility occupants (whether or not other employees or visitors are unaware of the organization's emergency management plans).

To be most effective, these immediate response measures must include all levels of employment as well as several teams established prior to the incident, many of which will remain active beyond the organization's response efforts and into its short- and long-term recovery. In addition to the above emergency management efforts, an organization should establish the following responsibilities.

Communications Responsibilities

Accurate and timely communication during incident response is vital for an organization to receive adequate aid from emergency services and law enforcement. It is also used to provide valuable, practical information such as known facts about the incident, road closures, and available resources for those affected. Additionally, employees' family members must be contacted and kept informed. Organizations must plan to ensure their communications during this difficult time are accurate, consistent, and helpful to all involved, including the following responsibilities:

- Individuals assigned by the EAP, as well as any on-site security personnel, must communicate with emergency services and law enforcement.
- HR, whether in-house or outsourced, must keep employees and their families informed.
- The organization's C-suite executives, legal team (in-house or outsourced), External Affairs (EA) team (if present), and employees assigned to a crisis communications team must communicate with the media.

While each communications avenue will be different, all communications efforts need to be coordinated as a whole.

Emergency Response

Security personnel, or a designated employee, from the organization should coordinate with emergency services and law enforcement to ensure adequate emergency response. Security personnel should make a predetermined communication plan that is available to all agencies that may respond to an active assailant incident (e.g., law enforcement, emergency services). They also must be prepared to communicate with police and emergency services personnel spokespeople upon their arrival and assist in incorporating these organizations' procedures as quickly as possible (e.g., where they need to be, where they can treat victims, pre-made routes for arriving and exiting).

These personnel must work with responding law enforcement and medical personnel to identify any employees not accounted for at the relocation area, hospitals, or morgue, and should be able to confirm if any employees were absent, traveling, working from home or from another facility, etc. They should also account for any non-employees in the building (e.g., guests, clients, suppliers, maintenance crews, deliverers).

Information Facilitation

Following an incident, different information should be given—and in different ways—to employees and their families, the media, and law enforcement. Disseminating the right information to the appropriate channels can be a daunting task and will require organization-wide coordination.

Organizations should consider using mass-communication technology to be able to send staff-wide alerts and updates so employees can take immediate action. This system should be established and practiced before an incident, with specific authorized personnel responsible for initiating these notifications. Individuals responsible for this communication should create pre-scripted messages that can be adapted and sent quickly in the event of an emergency. They should also set up these alerts on multiple channels (e.g., via cell phone and email) in case some methods of communication are temporarily unavailable.

Beyond organization-wide communication, HR personnel should communicate practical information to employees and their families, such as known facts about the incident, road closures, resolution and facility status, and appropriate assistance and accountability notifications. If an organization has no established HR personnel, this responsibility may fall to facility or company leadership, depending on the organization's structure. Again, they should be prepared to reach out using multiple communications channels if needed. Prior to the incident, HR should create and maintain a checklist of necessary and appropriate information to distribute and announce to staff and families—this checklist, like the organization's pre-scripted messages, should be updated accordingly in the wake of the incident.

Law enforcement is typically responsible for death notifications, but all organizations involved should understand their responsibilities and how to convey news accurately and compassionately. Personnel should be prepared to update family members directly about the incident, including potentially about missing, injured, or dead employees.[13] Information about missing, injured, or dead employees or similarly sensitive news should be delivered in an enclosed, private setting (e.g., a separate room of the organization's relocation center, if possible). An organization may be required to contact coroners or chaplains in the case of employee death.

As stated, HR personnel are responsible for facilitating accurate and timely information regarding an incident. However, misinformation can present obstacles to effective information sharing. Misinformation can spread quickly, causing rumors to undermine facts. HR personnel should have a plan in place for when and how they plan to control rumors that undermine post-incident efforts by the organization. This can include creating a statement template that summarizes the rumor and provides an explanation debunking the rumor.

Media

Organizations should create a crisis communications team to coordinate with the media—this team should include C-suite executives as well as the organization's legal team and EA department, if applicable. This team will develop and release information about the incident to the media, incident personnel, and other organizations, as appropriate. Contacts and working relationships should be established with local media prior to an incident. Additionally, the individual or team should develop standard talking points ahead of time for the organization's leadership to use when engaging with the media, using uniform, plain language. Legal and EA personnel should work together to ensure nothing is said that could cause issues for the company.

Depending on the organization's size and resources, this may be an internal communications team or a third-party hire. Regardless, this individual or team must have a direct line to the organization's C-suite executives. Companies may decide to hire or have on retainer a crisis management firm that specializes in handling incidents in terms of legal and communications issues.

IT Responsibilities

Taking a more proactive approach when addressing response procedures minimizes confusion and lapses in judgment during and immediately after an incident. Depending on the severity of the incident, local cell towers

[13] FBI, *Developing Emergency Operations Plans: A Guide for Businesses,* March 2018, https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view; CISA ISC, *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide,* November 2015, https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide.

may be overwhelmed with volume, limiting communications. Because of this, different channels may need to be temporarily used, such as providing updates on the organization's website or social media pages or using automated information lines to inform callers of the situation. The organization's IT professionals (whether in the company's own IT department or through a third-party service) should plan to use these communications channels and prepare to adapt them as needed during incident response.

Those operating company communications channels should be mindful that in the immediate wake of an incident, an organization, its employees, and its community may be targeted by spam and phishing attempts. These could take the form of websites, social media posts, crowdfunding platforms, or solicitations from spammers posing as charities. Fraudulent contractors may also contact the organization or its employees in an attempt to commit insurance fraud.[14] Organizations should do thorough research prior to signing any contracts, hiring outside aid, or donating money, and encourage employees to do the same; the U.S. Internal Revenue Service (IRS) charity database is a useful resource.[15]

IT, in coordination with the EA team, HR, or other relevant department, should warn personnel and the public of these risks (e.g., through social media posts, a warning on the company's website, or email notifications to employees and company partners).

Make employees aware of potential scams and fraud:

- Fraudulent donation requests may come from in-person solicitations, phone calls, emails, or social media.
- The IRS maintains a list of tax-exempt charities. A charitable organization that does not appear on this list may be fraudulent.
- Some fraudulent charity names may closely resemble those of recognized charities, or they may claim an affiliation with an existing charity.

Ensure that employees are provided a link to or list of recognized charities they can safely donate to.

Reiterate to employees the need to check websites and email addresses for anomalies that may indicate fraud.

[14] Federal Bureau of Investigation, "Charity and Disaster Fraud," accessed August 15, 2023, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud.
[15] U.S. Internal Revenue Service, "Tax Exempt Organization Search," accessed November 18, 2023, https://www.irs.gov/charities-non-profits/tax-exempt-organization-search.

Part Two: Short-Term Recovery

An organization's **short-term recovery** efforts should begin once the immediate concern of death, injury, and damage has passed. Short-term recovery, which can extend from days to weeks to months following the incident, is concerned primarily with ensuring the health and safety of the organization's employees and the resumption or continuation of business operations.

In the wake of an active assailant incident, an organization will be unrecognizable. Operations will not resume as usual once emergency services and law enforcement have left the scene. Depending on the severity of the incident, operations may not resume—in part or in whole—for weeks or even months. In addition, physical and mental trauma will take a great deal of effort to address, and an organization should be aware that no matter how well it responds to employees' needs after an incident, they may still be unwilling or unable to return to work.

Helping an organization and its employees begin to recover will involve many of the teams and processes created during the immediate response phase, as well as new teams and efforts undertaken by other members of the organization.

C-Suite Responsibilities

The responsibilities of C-suite executives extend far beyond their organization's initial response and into its short- and long-term recovery efforts. In the days and weeks following an incident, employees will be facing significant upheaval in both their personal and professional lives, and it is vital for the executive team to play an active role in their company's first steps to recovery.

C-suite executives play a pivotal role in disaster recovery and business continuity. They should take proactive measures, coordinate closely with each other and the rest of the organization, and prioritize not only business continuity but also the safety and health of their employees. Additionally, C-suite executives are responsible for effectively guiding the various departments they oversee to minimize both short- and long-term damage to the organization during a crisis. All decisions related to information and communication regarding the incident should be directed through the leader of the crisis/incident team.

The C-suite should also oversee the return of employees' belongings left behind during the evacuation process. They should inform all personnel that their belongings cannot be retrieved until the crime scene investigations are complete. In coordination with law enforcement, the C-suite should establish a central point for collecting personal belongings and ensure the items (many of which may be expensive and targets for theft, such as cell phones, wallets, and computers) are securely stored and guarded.

Communications Responsibilities

As with the C-suite, the communications team's responsibilities extend beyond the immediate crisis response stage and into short-term recovery. This team should continue to oversee necessary updates to the organization's website and/or social media channels to ensure their clients, partner organizations, and employees' loved ones are informed of ongoing safety and business continuity concerns.[16]

The communications team should establish a communication strategy that provides accurate and timely information throughout the early stages of the short-term recovery process. Not every organization may be robust enough to have a full crisis/incident management team, so there should be at least one appointed individual that can oversee the post-incident communication responsibilities. The individual or communications team must coordinate with C-suite management and leadership to appropriately distribute content and updates that highlight the organization's proactive efforts to handle the incident while also maintaining the organization's public image and business continuity plan.

[16] DHS, ready.gov, "Crisis Communications Plan," accessed July 13, 2023, https://www.ready.gov/crisis-communications-plan.

The communications team should also ensure that victims' families do not learn information about the incident via public channels before being told by the organization privately. In addition, the organization can consider setting up a hotline that employees and their loved ones can call to receive updates and access to relevant resources.

IT Responsibilities

The organization's IT service will need to determine if key facility IT and/or telecom equipment was damaged or disabled during the incident. It could take days to weeks for this equipment to be repaired and fully operational again. However, organizations can ensure this aspect of short-term recovery is conducted as smoothly and efficiently as possible by implementing thorough risk-preparedness measures (i.e., redundant systems, off-site recovery files, etc.) long before the recovery process is needed.

The primary function for an organization's IT service is to coordinate and provide context and information related to the IT impacts associated with the initial event or short-term recovery actions. IT should utilize risk assessment efforts shortly after an incident occurs, including a full system characterization, threat and vulnerability identification, control and impact analysis, and an immediate risk determination for ongoing short-term recovery mitigations.

Legal Responsibilities

A team should be established to manage the legal responsibilities for the organization following an active assailant incident. This team should consist of the organization's existing legal team (either onsite or on retainer) that oversees legal matters for the organization. To properly navigate any litigation that may arise, the organization may also need to establish partnerships or connections with external legal agencies or organizations before an incident occurs.

Litigation is a potential consequence following an active assailant incident, whether civil (e.g., negligence or wrongful death suits) or criminal. This team should be prepared to speak for the organization during litigation, which includes being able to accurately describe the incident and its outcomes, understanding what can be revealed publicly and what must be kept private, and properly dealing with media attention before, during, and after litigation.

The legal and communications teams should coordinate closely to ensure any information they are conveying publicly is legal, accurate, and up to date; their description of the organization itself is aligned with the organization's image; and their social media presence (both the organization and the individual) remains appropriate and does not unlawfully reveal information about the incident that should not be made public.

Additionally, traumatized victims may need free, capable legal support in processing potential legal responsibilities following an incident and during the ongoing investigation. The organization should consider a pre-developed victim legal plan in which the victims' legal needs are addressed.

Business Continuity Responsibilities

Continuing business operations after an active assailant incident will be challenging, if not impossible. Obstacles can include temporary or permanent loss of workplace access; a temporary or permanent diminished workforce due to dead, injured, traumatized, and/or grieving employees; loss of supplies or damage to workplace equipment/technology, including IT equipment; and supply chain disruption (both up and downstream). The facility will remain a crime scene under investigation potentially for an extended period; organization leaders should expect these disruptions to be similarly expansive and plan accordingly.

An organization must establish and exercise a thorough continuity of operations (CONOPS) plan long before an incident occurs to ensure essential business functions are still carried out post-incident.[17] Because traumatized and injured employees may not be able to resume their previous work for a long time, if ever, organizations need a plan for capable personnel to continue operating the facility, when possible.

Organizations should develop and enact a transition plan for resuming normal operations as quickly and smoothly as possible, which may include transitioning to a temporary workspace until normal offices or factory floors become operable or roads to/from the workspace are reopened. Capable personnel should be assigned, trained, and prepared to manage operational relocation or reorganization all while considering that some facilities may be inaccessible while law enforcement completes its investigation. Organizations should also plan for redundancy in critical communications, including IT services, at alternative sites, potentially utilizing the communications channels of stakeholders or other organizations up or down the supply chain.[18]

Ensuring that these business continuity measures are communicated throughout the entire organization, from top to bottom, is critical. Employees at every level of the organization should be involved to ensure that these short-term recovery procedures are comprehensive and efficient.[19]

Physical Security for People, Facilities, and Assets

Physical security is a vital part of any security plan. An organization's physical security and physical technology play particularly important roles not only in protecting personnel but also in ensuring effective and efficient future business continuity plans. An organization's physical technology (from computers and manufacturing equipment to existing physical security systems) may be intentionally targeted by an assailant or damaged or destroyed unintentionally during an attack. It is critical for organizations to develop guidelines to address potential damage, plan for systems to be replaced or repaired as quickly as possible to ensure business continuity, maintain their brand and reputation, and ensure the protection of their employees, customers, and business.

HR Responsibilities

Employees will face significant upheaval and post-disaster distress following an active assailant incident and will need all resources available to them and the support of their organization throughout recovery.[20] An organization's HR department (whether internal or outsourced) may perform or be assigned multiple roles during the initial stages of short-term recovery, including:

- Handling employee deaths and insurance payouts for families.
- Managing deceased employees' personal items for families and ensuring they are appropriately returned.
- Navigating absences due to injury or emotional trauma.
- Connecting employees to mental health services through an Employee Assistance Program.
- Navigating payroll, sick leave, and medical benefits if employees are unable to return to work for an extended period or never able to return to work, etc.

---

[17] Federal Emergency Management Agency (FEMA), *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101,* September 2021, https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf.
[18] CISA, *Critical Manufacturing Sector Security Guide,* July 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.
[19] CISA, "Active Shooter Emergency Action Plan Product Suite," accessed on July 12, 2024, https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite.
[20] Substance Abuse and Mental Health Services Administration, "Disaster Distress Helpline," accessed July 12, 2023, https://www.samhsa.gov/find-help/disaster-distress-helpline; VictimConnect, "VictimConnect Resource Center," accessed July 12, 2023, https://victimconnect.org/; FBI, "FBI Victim Services," 2018, https://www.fbi.gov/file-repository/fbi-victim-services-brochure-2018.pdf/view.

- Managing stress control for employees, such as potentially offering time off for employees who have been overseeing the organization's crisis management efforts.
- Managing any memorial candles or other items left at the location(s) to honor any deceased and/or injured. These items will also need to be managed after the incident, and the burden should not fall to the public.
- Considering local nonprofit organizations that can manage and distribute donations made by the public following an incident.
- Working alongside the communications team and C-suite management to acknowledge and address employees' concerns post-incident.

Part Three: Long-Term Recovery

The **long-term recovery** phase consists of activities that continue far beyond the incident period and focuses on restoring, redeveloping, and revitalizing critical organizational and community functions and beginning to manage stabilization and mitigation efforts. Be aware that the full recovery process will take years to complete. Conducting a comprehensive after-action review is critical to preparing for future incidents, whether human-caused or natural. This review should be done in concurrence with long-term recovery efforts and can be incorporated into the after-action review and follow-on documentation.

Many of the measures undertaken in Parts One and Two must be continued in the long term, often adapting and expanding far beyond the initial team structures described above. There may also be an overlap between some short-term and long-term recovery activities. These long-term efforts must focus on ensuring the health, safety, and stability of an organization's employees as well as support business continuity, the organization's standing with the media and public, and the organization's long-term cyber and physical security.

Employee Health Responsibilities

Both HR and high-level management will have many ongoing responsibilities during an organization's long-term recovery. It is vital that the company continue to provide for and accommodate their employees' changing physical and mental health concerns, many of which will extend into the long term.[21]

Trauma affects people in different, often unexpected ways. Employees may be anxious or feel unsafe in certain scenarios, and the company should be ready to accommodate these changes. For example, small, enclosed spaces (such as a closed office door) may trigger a sense of fear.

The company may need to expand its existing healthcare provisions to ensure employees' physical health and security. The company may also seek to partner with outside mental health services to adequately meet employees' mental health needs. This could include providing grief counseling to help employees cope with the long-term effects on their mental wellbeing.

In addition to supporting their employees' physical and mental health concerns, the organization will need to identify and recognize employees who have been harmed or who have passed away. Families and coworkers will likely want to commemorate the event in some way on the facility property either via a ceremony, a physical memorial, or both. This may occur annually as well.

Business Continuity Responsibilities

Restoring and maintaining business operations will remain a challenge in the months and years following an incident.[22] An organization should consider several components when addressing potential business continuity issues such as long-term supply chain disruptions;[23] long-term or permanent employment loss due to injury, trauma, or safety concerns about returning to the facility; and potential economic and branding impacts to the organization. The organization should review and evaluate all components within its supply chain to determine any factors that influence its ability to reestablish supply into the market.

As noted in Part Two, an organization will inevitably face employment loss in the aftermath of an active assailant incident, and in many cases, this diminished workforce will extend into the long term. Organizations should recognize that some employees may never want to return to the same environment or resume

---

[21] CISA ISC, *Violence in the Federal Workplace: A Guide for Prevention and Response,* 2019, https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide; DHS, *Active Shooter Recovery Guide,* August 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide.
[22] DHS, *Active Shooter Recovery Guide,* August 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide.
[23] CISA, *Critical Manufacturing Sector Security Guide,* July 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.

operations, even at a different location. The psychological and physical impact of such a traumatic incident is different for everyone. To maintain employment levels as best as possible and ensure that existing employees remain with the company, the organization must understand and accommodate the variety of reasons employees are unable or unwilling to return to work. Some employees may have sustained physical injuries that will last into the long term. Others may still be unable to work due to ongoing trauma, grief, or fear of returning to an unsafe work environment.

Note that safety concerns, as well as the social and professional stigma that may arise around the organization following an incident, may keep both existing employees as well as prospective hires away. To retain existing employees and attract new personnel, the organization must prepare to accommodate their needs. For example, organizations can improve and increase security systems, closed-circuit televisions (CCTVs), and security training procedures to ensure that the building is safe for return for all existing and potentially new employees.

Companies will need to actively provide and coordinate ongoing support for any employees with existing trauma and provide mental health services to adequately meet employees' mental health needs. Additional funding may be required to accommodate counseling and mental health services for employees on a permanent basis.

In addition, organizations will need to review and analyze any long-term economic impacts post-incident to both ensure the economic health of the company and maintain their brand and reputation within the industry, supply chain, and community. Reputational damage can be assessed by examining the company's market share and stock price. As part of their economic analysis, the company will need to consider extended compensation claims and other types of financial assistance for their employees which may extend into the long-term recovery period.

Public Outreach Responsibilities

The organization's communications responsibilities will continue into the long term as well. Efforts from the communications team, legal team, C-suite executives, and others will need to handle ongoing interactions with law enforcement, emergency services, and any legal proceedings that may arise. They may also be tasked with keeping the organization's website and social media presence up to date to convey information about the recovery process. This may include details about new security measures, condolences for anyone injured or dead in the incident, and business continuity updates. Additionally, it is crucial for the organization to maintain a separate communication channel specifically for employees who were directly impacted by the incident and their loved ones. This ensures that they receive the necessary support and information during the long-term recovery process.

Additionally, the organization will need to plan for annual remembrance events and memorials. These are opportunities to reassess the organization's security and planning needs and determine the health, security, and stability of employees. They also acknowledge the impact an incident has had on a company, its employees, their families, and the community. Depending on the magnitude of the incident, these remembrance events may also necessitate coordinating a statement or event with the press, in addition to making a statement on the organization's website and social media pages.

Cyber and Physical Security Responsibilities

Restoring the security of an organization following an incident—including both the safety of employees and the cyber and physical security of its assets—is a vital piece of long-term recovery that may take months or even years to achieve. There are several factors that an organization needs to consider as a part of their cyber and physical security responsibilities. The organization must analyze all physical and cyber damage inflicted from

the incident,[24] which includes insider threat possibilities, stolen or damaged personal items, compromised physical security/cybersecurity systems, and destroyed or compromised physical and electronic assets. This also includes any damage or change to the organization's reputation within the industry, the supply chain, and the community.

Addressing these damages is essential not only for safeguarding the organization's business continuity and financial security but also for enhancing employees' feelings of security within the organization. Many workers will feel unsafe returning to a location that has been compromised in the past—even after months or years have passed—and will need to see tangible and meaningful changes to the organization's security measures. Involving employees in discussion about the necessary improvements, as well as soliciting their input on what they saw during the incident that could have been prevented or mitigated, can be a valuable step in implementing these changes. These changes may include installing an up-to-date, comprehensive security system at all entrances/exits to the building, multi-factor authentication for all company data, and mandatory active assailant training for all employees, covering prevention, mitigation, and response/recovery.[25] If the organization already had training in place prior to the incident, an evaluation of the program may be needed to make sure it is up to date. Because technology is advancing at such a rapid rate, even a new training program may need to be updated to account for changes in cybersecurity threats and the ways that security systems, machinery, and data can be compromised.

Recognize that for some employees who have experienced previous trauma, certain training plans and exercises may be difficult or impossible due to the emotional distress caused by the content of the training. For these employees, be understanding and compassionate, and look for alternate ways (e.g., different training programs, written instructions instead of video) to keep them up to date on the organization's security measures and emergency procedures.

Many federal resources exist to inform and train organizations and their employees on cyber and physical threat detection, prevention, and mitigation. These include CISA's suite of insider threat mitigation resources[26] and their Insider Risk Mitigation Program Evaluation (IRMPE), which can be used to gauge an organization's readiness for an active assailant incident.[27] Other online training courses, such as FEMA's various disaster preparedness courses, should be required for employees to strengthen their emergency preparedness skills.[28] These steps should be performed regularly to ensure an organization's safety and cyber-physical security.

---

[24] CISA, *Critical Manufacturing Sector Security Guide,* July 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.
[25] CISA ISC, *Violence in the Federal Workplace: A Guide for Prevention and Response,* 2019, https://www.cisa.gov/sites/default/files/publications/isc_workplace_violence_guide_-_2019_0.pdf.
[26] CISA, "Insider Threat Mitigation," accessed July 13, 2023, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation.
[27] CISA, "Insider Risk Mitigation Program Evaluation (IRMPE)," accessed July 12, 2023, https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe.
[28] FEMA, Emergency Management Institute, "ISP Courses," accessed July 13, 2023, https://training.fema.gov/is/crslist.aspx?lang=en.

Conclusion

The CM Sector Active Assailant Post-Incident Best Practices Guide serves as a resource for critical manufacturing organizations of all sizes. All critical manufacturing organizations and affiliates can use this Guide when planning their post-incident response and recovery efforts.

Even if an organization takes all the steps presented in this Guide when an incident occurs, employees are unlikely to ever return to their pre-incident levels of comfort and security within the organization. Similarly, the organization may excel in its business continuity efforts and still never reach its pre-incident operation levels.

Remember that recovery is not a linear process, and the impacted organization may never return to its pre-incident normalcy. However, by using these steps as a guide for immediate response, short-term recovery, and long-term recovery, **the organization may achieve a new baseline in assuring the safety of employees and continuity of its operations.**

For more information or to seek additional help, contact us at CriticalManufacturingSector@cisa.dhs.gov.

Appendix A: Tear-Out Sheets

This Appendix provides a series of checklists for critical manufacturing organizations and affiliates to prepare their immediate response, short-term recovery, and long-term recovery plans in the wake of an active assailant incident. These checklists are designed to be separated from the Best Practices Guide and printed and distributed as needed among the C-suite executives, Human Resources (HR) personnel, and all other employees involved in the creation and execution of the company's Emergency Action Plan (EAP).

Organizations should tailor these lists to their specific circumstances and resources, use them during active assailant incident training, keep them on hand when possible during incident response and recovery, and update them as needed after an incident or to reflect any changes in their company structure or EAP.

Before an Incident Happens

Use this list to ensure that your company's EAP is comprehensive, up to date, and tailored to your organization's building(s), employment structure, and location. Alter the titles and employment categories as needed and indicate any positions that will need to be outsourced, as well the designated individual(s) within your company responsible for contacting and maintaining a connection with these outsourced groups pre-incident.

Immediate Assembly Accountability

Use these checklists to ensure designated employees keep an accurate and thorough record of all organizational personnel and their status during and after an evacuation. If needed, add more rows to the table and include separate columns for other locations specific to your EAP.

Immediate Response

This list outlines the basic responsibilities required of various positions within an organization, including the C-suite, Security Director, HR, and legal team, to carry out a streamlined and secure immediate response effort. Adjust these positions as needed to fit your organization's structure and tailor individual responsibilities to fit your organization's EAP.

Short-Term Recovery

As with the above, use this checklist to cover the basics of your organization's short-term recovery plan, adjusting roles and responsibilities as needed to fit your company's structure and situation. Note any procedures that will need to be outsourced, as well as a means of contacting and maintaining a working relationship with these services and the individual(s) within your company responsible for contacting and working with them post-incident.

Long-Term Recovery

Use this list, as with the above, to outline your company's long-term recovery efforts. Consult this list periodically during the months and years of your long-term recovery, updating and adjusting it as needed to reflect any changes in circumstances or new areas of focus (e.g., advancement in litigation, changes in personnel's health or employment status, fluctuations in the company's financial situation).

Before an Incident Happens

Security Director/Facility Director

- Develop and implement an Emergency Action Plan (EAP). See www.ready.gov for ideas and templates, as well as the Business Continuity Planning Suite.
- Coordinate with local first responders (police and fire) to identify a process to gain accountability of personnel, methods of securing company areas, what to expect during and after an incident, and how and when to get personal belongings back to employees.
    - Purses, IDs, computers, phones, cars, etc., will likely be left behind in the evacuation and will need to be secured and guarded prior to an orderly pick-up by employees and/or next of kin.
- Coordinate with fire rescue and medical first responders on triage needs. Identify and map out medical and trauma centers in the area.
- Train staff in evacuation procedures.
    - Ensure your evacuation procedures are practical for any personnel with access and functional needs or who may not be fluent in English.
- Create a multi-channel (e.g., phone, email) employee notification system and assign responsibility for its activation.
    - Conduct periodic tests of this notification system, ensuring it reaches all employees regardless of any disability, language barriers, or work areas with high noise levels.
- Provide/utilize training in the National Incident Management System (NIMS).
- Use federal resources such as the Office for Victims of Crime toolkit, Federal Emergency Management Agency (FEMA) preparedness guide, and Occupational Safety and Health Administration (OSHA) Emergency Action Plan eTool.
- Establish an accountability group and predetermine methods of accounting for personnel (e.g., app check-in).
- Appoint qualified employees to a medical operations group, if possible.
- Establish a utility security group if necessary.
- Implement and practice a comprehensive Continuity of Operations (CONOPS) plan.
- Encourage employees to receive training in first aid and CPR.
- Establish lead assembly persons for all floors, facilities, and other locations to track and report accountability.

Human Resources (HR)

- Work with the Security/Facility Director to know where medical and trauma centers are located. Ensure all points of contact (POCs) at locations are up to date and introductions have been made (e.g., hospital communications staff).
- Work with your legal team, External Affairs (EA), C-suite, and other relevant parties to identify and arrange assembly and relocation areas and secure required contracts (hotels, conference centers, etc.) to be implemented when needed.
    - Ensure these parties are kept up to date with current POCs and any updates to the EAP.
- Determine employee requirements and benefits in the event of such incidents, including the company's responsibilities.
- If a union is in place at facility, work with union representatives and employees to identify and address any union issues that need to be considered.
- Create and maintain a checklist of essential information to be communicated to employees and their families in case of an incident.

Employees

- Complete company-provided active assailant training.
- Participate in company-provided active assailant exercises.
- Participate in employee notification system tests and provide feedback.
- Ensure all POC, next of kin, etc., information is kept up to date.

- Ensure all medical and insurance beneficiary and other information is kept up to date.
- Ensure family members have access to copies of all medical and insurance information in an easily accessible location in case of emergency.

Legal

- Work with C-suite, HR, the Security Director, and other relevant parties to address legal issues related to potential incidents.
- Work with EA and C-suite to develop media talking points in case of an incident, ensuring that no statements are made that could pose problems for the company.

External Affairs/Communications

- Work with C-suite, HR, the Security Director, etc., on messages to send to impacted families and employees.
- Formulate mainstream and social media and outreach templates to facilitate reporting. Being ahead of the issue can prevent misinformation from being front and center in the media/online.
- Establish a crisis communications team to handle media relations, disseminating incident-related information to all relevant parties as required.
- Build connections and cultivate working relationships with local media outlets.
- Work with C-suite, HR, the Security Director, IT, and any other relevant groups to establish messaging templates for potential fraudulent donation websites, solicitations, etc. Be prepared to combat such activities by regularly publishing/announcing accurate donor information.

Information Technology/Network Group

- Work with the Security Director to safeguard the company's cybersecurity and cyber assets during physical incidents.
- Maintain continuous network integrity.
- If needed, assist in setting up an employee notification system.
- Plan to use alternate communications channels such as social media and company websites for communication and prepare to adapt them as needed during incident response.
- Establish plans for potential threat actors to take advantage of a degraded network system during an incident.

Finance/Contracting/Vendor

- Incorporate contract clauses to address human-caused incidents.
- Follow up with vendors and clients to assess any pending purchases or orders.

Immediate Assembly Accountability

- **Make note of and triage injured personnel for emergency medical responders.**
- **If applicable, use pre-established methods to transport employees to safety.**

Following an evacuation, members of the designated accountability group must take accountability of personnel, including the total number of individuals in each category as well as their names and location (if known).

Accountability Group:
Floor/facility/area managers or other employees pre-designated to account for personnel (including injured, well, missing, traveling/out of town/on leave) after evacuation

Accounted for, Off-Site (traveling, out of town, on vacation, etc.)	**Well**	**Injured** (include hospital and/or status, if known)	**Missing/Unknown**
Total #:	**Total #:**	**Total #:**	**Total #:**

Immediate Response

Security Director/Facility Director

- Coordinate with local first responders.
- Ensure that C-suite, HR, External Affairs (EA)/communications team are informed about the medical facilities where employees have been taken.

C-Suite

- If the facility is still operational, discuss when and to what extent operations can resume after investigations.
- Reach out to employees, families, customers, and stockholders affected by the incident.
- Work with EA/communications to handle media coverage of the incident.

Human Resources Team

- Work with the Security/Facility Director to identify the medical facilities where employees have been taken.
- Work with your legal team, EA, C-suite, and other relevant parties to arrange relocation areas (hotels, conference centers, etc.).
- Keep employees and their families informed about the status of the incident and the whereabouts of employees.
- Initiate any required documentation for affected employees who may be unable to work due to injuries or for the families of deceased employees.
- Work with union representatives, if applicable, to ensure the organization adheres to union requirements and to address any potential union-related issues due to incident.
- Work with mental health professionals to create plans for immediate and long-term trauma support, including addressing post-traumatic stress.
- Communicate necessary information to employees and their families, such as confirmed details about the incident, road closures, facility status updates (including picking up personal belongings), and appropriate assistance and accountability notifications.
- Accurately, compassionately, and privately update family members directly about the incident, including about potentially missing, injured, or deceased employees.

Legal Team

- Work with C-suite, HR, the Security Director, and any other relevant groups to prepare for any legal issues that may arise from the incident.

IT Team/Network Group

- Work with the Security Director to safeguard the company's cyber assets from any potential impact caused by a physical incident.
- Maintain network integrity.

External Affairs Team/Communications

- Work with C-suite, HR, the Security Director, and other relevant groups to develop and communicate messages to families and employees who have been affected by the incident. This may include developing pre-scripted messages to assist with communication in the immediate aftermath of an incident.
- Continue overseeing communication with the media until the incident has been fully resolved.
- Message legitimate charities for donations. Advise people to be aware of fraudulent charities and to report them appropriately.

Short-Term Recovery

Security Director/Facility Director

- Identify lessons learned from security successes and failures.
- Incorporate lessons learned and update the organization's Emergency Action Plan (EAP).

C-Suite

- Repair any damage sustained by the facilities during the incident.
- Ensure that the facilities are safe for employees to return to work.
- Provide reassurance to shareholders in the event of a market drop.

Human Resources Team

- Develop a plan to facilitate the transition of employees back to work.
- Consider the potential impact of trauma on employees' ability to return to work.
- Determine how to appropriately handle items left at the facility, whether they are returned to employees, family members, or used as part of a memorial.
- Decide whether the company will organize memorial services on the incident's anniversary.

Legal Team

- Handle lawsuits from injured and/or deceased employees' families.
- Manage any legal proceedings related to the suspect(s).
- Prepare to represent the organization during litigation, including accurately describing the incident and outcomes, managing public disclosures, and handling media throughout the legal process.
- Explore the possibility of having a pre-established legal support plan in place to address the needs of the victims.

IT Team

- Determine whether any IT and/or telecommunications equipment has suffered damage or disruptions due to the incident.
- Conduct cyber and/or IT risk assessments shortly after the incident occurred.

External Affairs/Communications Team

- Continue to communicate with employees and navigate any media requests.
- Offer precise and timely information during the initial phases of short-term recovery.
- Coordinate with C-suite leadership to share updates on your proactive incident management while preserving your public image and business continuity plan.
- Establish a hotline that employees and their loved ones can call to receive updates and/or access with relevant resources.
- Work with HR to identify and provide resources employees and next of kin can use if needed (medical, psychological, etc.)

Finance Team/Contracting/Vendor

- Follow up with vendors and clients to assess impacts pending purchases or orders.
- Work to obtain costs for short- and long-term recovery, including cleaning and repairing of facilities, adding new security measures based on lessons learned, expanded healthcare or other employee benefits, etc.

Long-Term Recovery

Security Director/Facility Director

- Incorporate lessons learned into incident training and exercises.
    - Implement new or evaluate existing active assailant training programs for employees, to be conducted and updated regularly (e.g., annually).
- Update the organization's existing Emergency Action Plan (EAP).
- Implement new security protocols and technology based on lessons learned.
- Assess all physical damage post-incident, including stolen or damaged items, compromised security systems, and affected assets.

C-Suite

- Work to reestablish company reputation in the media, the industry, and your supply chain.
- Maintain contact with employees to assure them of the company's commitment to rehabilitation.
- Evaluate business continuity concerns, including extended supply chain disruptions, sustained employment challenges due to injury or trauma, and potential economic impacts.

Human Resources Team

- Provide resources for long-term mental health support for traumatized employees.
- Broaden employee healthcare to address post-incident health issues as needed.
- Administer and disburse insurance payouts to deceased employees' families.
- Adapt to accommodate employees' evolving physical and mental health needs.

Legal Team

- Address legal actions initiated by the families of injured or deceased employees.
- Handle any legal actions related to the suspect(s).

IT Team

- Update compromised systems as necessary.
- Assess all cyber and cybersecurity damage, including compromised systems and electronic asset loss.

External Affairs/Communications Team

- Update the organization's website and social media with recovery updates, security measures, condolences, and business continuity information.
- Expect and plan for memorials and remembrance events in the weeks, months, and years after the incident, potentially including coordinating a statement or event with media, employees, and loved ones of deceased.

Finance Team/Contracting/Vendors

- Follow up with vendors and clients to assess impacts pending purchases or orders (long term).
- Work to update all contracts, etc., as developed in plan and incorporate lessons learned.

Appendix B: Resources

Active Assailant Threat Guidance

- Active Shooter Emergency Action Plan Product Suite, Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite
- Shields Up! Cyberattack Resources, CISA: https://www.cisa.gov/shields-up
- Active Shooter Attacks – Action Guide, CISA: https://www.cisa.gov/resources-tools/resources/active-shooter-attacks-action-guide
- Vehicle Ramming – Action Guide, CISA: https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide
- Fire as a Weapon – Action Guide, CISA: https://www.cisa.gov/resources-tools/resources/fire-weapon-action-guide
- Chemical Attacks – Action Guide, CISA: https://www.cisa.gov/sites/default/files/2022-11/Chemical%20Attacks%20-%20Security%20Awareness%20for%20ST-CP.PDF
- Complex Coordinated Attacks – Action Guide, CISA: https://www.cisa.gov/resources-tools/resources/complex-coordinated-attacks-action-guide
- Protecting Against the Threat of Unmanned Aircraft Systems (UAS), CISA Interagency Security Committee (ISC): https://www.cisa.gov/resources-tools/resources/isc-best-practices-protecting-against-uas-threat
- Counter-IED Resources Guide, CISA: https://www.cisa.gov/sites/default/files/publications/obp-counter-ied-resources-guide.pdf
- What to Do – Bomb Threat, CISA: https://www.cisa.gov/news-events/news/what-do-bomb-threat
- Insider Threat Mitigation, CISA: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

Business Continuity Plan Guides

- Business Continuity Plan, U.S. Department of Homeland Security (DHS): https://www.ready.gov/business-continuity-plan
- Business Continuity Planning Suite, DHS: https://www.ready.gov/business-continuity-planning-suite
- Crisis Communication Plan, DHS: https://www.ready.gov/crisis-communications-plan

Emergency Action Plan Resources

- Developing Emergency Operations Plans: A Guide for Businesses, Federal Bureau of Investigation (FBI): https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view
- Emergency Action Plan Guide: Active Shooter Preparedness, DHS: https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite
- Are You Ready? Basic Preparedness, Federal Emergency Management Agency (FEMA): https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf
- Evacuation Plans and Procedures eTool, Occupational Safety and Health Administration (OSHA): https://www.osha.gov/etools/evacuation-plans-procedures/eap
- Emergency Response Plan, DHS: https://www.ready.gov/business/implementation/emergency
- Incident Management, DHS: https://www.ready.gov/incident-management

Emergency Assistance and Victim Support

- FBI Victim Services, FBI: https://www.fbi.gov/file-repository/fbi-victim-services-brochure-2018.pdf/view
- VictimConnect Resource Services, VictimConnect: https://victimconnect.org/
- Disaster Distress Helpline, Substance Abuse and Mental Health Services Administration (SAMHSA): https://www.samhsa.gov/find-help/disaster-distress-helpline
- Antiterrorism and Emergency Assistance Program, U.S. Department of Justice (DOJ) Office for Victims of Crime (OVC): https://ovc.ojp.gov/program/antiterrorism-and-emergency-assistance-program-aeap/overview

- Helping Victims of Mass Violence & Terrorism, OVC: https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/mvt-toolkit/victim-assistance.html
- National Mass Violence Victimization Resource Center (NMVVRC): https://www.nmvvrc.org/
- Technical Resources, Assistance Center, and Information Exchange (TRACIE), U.S. Department of Health and Human Services (HHS): https://asprtracie.hhs.gov/technical-resources
- Find Treatment, (SAMHSA): https://findtreatment.gov/
- Find a Health Center, HHS, Health Resources and Services Administration (HRSA): https://findahealthcenter.hrsa.gov/
- Charity and Disaster Fraud, FBI: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud

Personal Preparedness Resources

- Stop The Bleed®, American College of Surgeons: https://www.stopthebleed.org/training/
- You Are the Help Until Help Arrives, FEMA: https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US
- On-Site Group Training for Teams and Employees, American Red Cross: https://www.redcross.org/take-a-class/train-my-employees
- Online Safety Training Courses, American Red Cross: https://www.redcross.org/take-a-class/online-safety-classes/all-online-classes
- Attacks in Crowded and Public Spaces, DHS: https://www.ready.gov/public-spaces

Response and Recovery Planning Guides

- Active Shooter Recovery Guide, DHS: https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide
- Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide, CISA ISC: https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide
- Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101, FEMA: https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf
- Physical Security: Insider Threat Mitigation, CISA: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation
- Violence in the Federal Workplace: A Guide for Prevention and Response, CISA ISC: https://www.cisa.gov/sites/default/files/publications/isc_workplace_violence_guide_-_2019_0.pdf
- Mass Violence and Terrorism Resources, OVC Training & Technical Assistance Center: https://www.ovcttac.gov/massviolence
- Workplace Violence, OSHA: https://www.osha.gov/workplace-violence/enforcement

Sector Security Resources

- Critical Manufacturing Sector Security Guide, CISA: https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf

Security Training and Assessments

- National Incident Management System (NIMS), FEMA: https://www.fema.gov/emergency-managers/nims
- Independent Study Program (ISP) Course List, FEMA: https://training.fema.gov/is/crslist.aspx?lang=en
- Insider Risk Mitigation Program Evaluation (IRMPE), CISA: https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe
- Vehicle Ramming Self-Assessment Tool, CISA: https://www.cisa.gov/vehicle-ramming-self-assessment-tool