Après un incident impliquant un assaillant actif dans le secteur manufacturier essentiel

GUIDE DE BONNES PRATIQUES

JUILLET 2024

Ministère de la sécurité intérieure des États-Unis
Agence de cybersécurité et de sécurité des infrastructures

TABLE DES MATIÈRES

APERÇU 1

PREMIÈRE PARTIE : RÉPONSE IMMÉDIATE 2

Responsabilités des cadres dirigeants 2

Responsabilités de la gestion des urgences 2
Système de notification 3
Cheminements d'évacuation 3
Équipes d'évacuation 4
Équipes d'intervention médicale 5
Groupes de sécurité de l'infrastructure 6

Responsabilités de l'équipe de communication 6
Intervention d'urgence 7
Facilitation de l'information 7
Médias 8

Responsabilités du service informatique 8

DEUXIÈME PARTIE : RÉCUPÉRATION À COURT TERME 9

Responsabilités des cadres dirigeants 9

Responsabilités de l'équipe de communication 9

Responsabilités du service informatique 10

Responsabilités juridiques 10

Responsabilités de la continuité d'activité 10
Sécurité physique du personnel, des installations et des actifs 11

Responsabilités des RH 11

TROISIÈME PARTIE : RÉCUPÉRATION À LONG TERME 12

Responsabilités en matière de santé des employés 12

Responsabilités en matière de la continuité d'activité 12

Responsabilités en matière de sensibilisation du public 13

Responsabilités en matière de cybersécurité et de sécurité physique 13

CONCLUSION 14

ANNEXE A : FEUILLES DÉTACHABLES 15

ANNEXE B : RESSOURCES 22

APERÇU

Ce guide de bonnes pratiques après un incident impliquant un assaillant actif dans le secteur manufacturier essentiel sert de ressource pour les efforts de réponse et de récupération post-incident pour le secteur manufacturier et ses partenaires. La planification, la préparation et la mise en œuvre des processus essentiels de réponse et de récupération sont des étapes cruciales. Elles aident les manufacturiers essentiels et toutes les filiales à rester résilients face à un incident impliquant un assaillant actif.

Un **assaillant actif** est un individu qui s'emploie activement à tuer ou à tenter de tuer des personnes dans une zone peuplée[1]. Ces assaillants peuvent utiliser des armes à feu, un véhicule bélier, des bombes, des engins incendiaires, des armes chimiques, des drones ou d'autres méthodes. Lorsqu'une organisation est confrontée à un incident impliquant un assaillant actif, elle doit prendre deux mesures tout aussi importantes l'une que l'autre. La première est **l'intervention immédiate,** c'est-à-dire les premières mesures prises par le personnel après un incident pour sauver des vies et minimiser les dégâts. Une fois ces mesures prises, l'étape suivante, **la récupération**, commence, à la fois **la récupération à court terme** — rétablir la sécurité et atténuer les impacts physiques, psychologiques et émotionnels dans les jours, les semaines et les mois qui suivent l'incident ; et **la récupération à long terme**— aider l'organisation à reprendre ses activités et aider les personnes touchées à retrouver un sentiment de normalité dans leurs interactions quotidiennes et dans leur vie professionnelle, un processus qui prendra probablement des années. Il faut savoir qu'il n'y a pas de distinction nette entre ces étapes : la réponse immédiate se fondra dans les jours qui suivent un incident, tout comme la récupération à court terme se prolongera dans les mois qui suivent.

Les mesures décrites dans ce guide peuvent varier considérablement selon le type d'organisation (p. ex. un bureau par rapport à une usine, une seule société composé d'un bâtiment unique par rapport à une organisation répartie sur plusieurs sites ou une grande entreprise disposant de ressources importantes par rapport à une petite entreprise disposant d'un personnel limité). La taille d'une organisation a un impact particulier sur les efforts d'intervention et de récupération après un incident. Par exemple, les petites et moyennes entreprises peuvent demander à leur équipe de direction et à un nombre limité d'employés d'assumer de multiples rôles et responsabilités qu'une organisation plus importante pourrait répartir plus largement au sein de son personnel. Les petites et moyennes entreprises ne disposent pas forcément des mêmes ressources qu'une grande entreprise et peuvent souhaiter, ou doivent, externaliser certains des services mentionnés dans ce guide plutôt que de s'appuyer sur des mesures et du personnel internes. Les services concernés vont du service informatique au service juridique. Pour se préparer au mieux à un incident et assurer la sécurité des travailleurs et la continuité d'activité, une organisation doit prendre en compte les ressources disponibles, les employés, le ou les bâtiments et la nature de ses activités.

Par-dessus tout, un manufacturier essentiel doit effectuer ces préparatifs bien avant qu'un incident impliquant un assaillant actif ne se produise. En l'absence d'une planification adéquate, d'une délégation des tâches, de liens avec la communauté et d'une compréhension de l'impact considérable d'un incident impliquant un assaillant actif, il est peu probable que l'intervention et la récupération soient couronnés de succès.

Clause de non-responsabilité : *L'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) ne cautionne aucune entité, produit, entreprise ou service commercial, y compris les entités, produits ou services liés à ce document. Toute référence à des entités commerciales, des produits, des processus ou des services spécifiques par le biais d'une marque de service, d'une marque déposée, d'un fabricant ou autre, ne constitue pas ou n'implique pas une approbation, une recommandation ou un avis de favoritisme de la part de CISA.*

---

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

PREMIÈRE PARTIE : RÉPONSE IMMÉDIATE

La phase de **réponse immédiate** se concentre principalement sur les actions immédiates d'une organisation pour sauver des vies, réduire les impacts sur la santé physique et mentale, assurer la sécurité publique et répondre aux besoins des personnes touchées. Avant de commencer à réfléchir à la manière de se remettre d'un incident, une entreprise doit d'abord savoir comment réagir à l'incident lui-même. Une réponse efficace, efficiente et rapide repose sur la mise en place de mesures de préparation tenant compte des risques.

Les propriétaires et les exploitants doivent former le plus grand nombre possible de membres de leur personnel aux techniques de secours de base, telles que les premiers secours et la réanimation cardio-pulmonaire, qui peuvent être nécessaires avant que les services d'urgence n'arrivent sur les lieux d'un incident[2]. Cependant, pour une navigation efficace des étapes complexes et sensibles au facteur temps requises pour une intervention immédiate, il faut une approche plus organisée à l'échelle de l'entreprise, qui comprend la définition et la délégation des responsabilités suivantes, en commençant par le sommet de l'organisation.

RESPONSABILITÉS DES CADRES DIRIGEANTS

Les dirigeants de haut niveau, souvent appelés cadres dirigeants, jouent un rôle essentiel dans l'élaboration, l'engagement et la mise en œuvre des mesures d'intervention en cas d'incident au sein de leur organisation. Face à une situation d'urgence, les employés se tournent vers les dirigeants de l'organisation pour obtenir des conseils. Les cadres doivent participer et jouer un rôle actif dans la mise en œuvre des plans de l'entreprise, des cours de formation ou des mesures de sécurité. Ils doivent prendre l'initiative de ces efforts pour le reste de l'organisation.

Si les dirigeants sont dédaigneux et mal informés au sujet des assaillants actifs ou d'autres menaces, leurs employés seront plus susceptibles d'adopter le même état d'esprit. Inversement, si les employés constatent que les dirigeants de haut niveau s'engagent à élaborer et à mettre en œuvre un plan d'action d'urgence (PAU) complet, ils sont davantage susceptibles de prendre la menace au sérieux. Si les dirigeants d'une entreprise sont paniqués ou indécis face à un incident, leurs employés risquent de réagir de la même manière. Mais si les dirigeants sont confiants, décisifs, compatissants et informés pendant et après un incident, leurs employés seront plus enclins à suivre leur exemple et à mettre en œuvre des mesures d'urgence efficaces.

Les dirigeants de haut niveau doivent participer activement à la planification et à l'exécution de ces mesures. Cette participation peut prendre diverses formes, comme l'organisation ou l'attribution de cours de formation réguliers sur la gestion des urgences et les premiers secours ou encore la diffusion d'informations sur les mesures à prendre en cas d'incident sous la forme de dépliants, d'affiches ou d'autres lignes directrices accessibles dans leurs installations ou leurs bureaux.

RESPONSABILITÉS EN MATIÈRE DE GESTION DES URGENCES

La création d'un PAU est la mesure la plus importante qu'une organisation puisse prendre pour mettre en œuvre une réponse immédiate transparente, efficace et efficiente. Il doit s'agir d'un plan qui concerne l'ensemble de l'organisation et qui implique tous les employés (y compris les cadres dirigeants, comme indiqué ci-dessus). Face à un incident impliquant un assaillant actif, tous les membres du personnel doivent se voir assigner un rôle qu'ils connaissent bien et qu'ils maîtrisent afin de garantir leur sécurité et celle du reste de l'organisation. En fonction de la taille de l'organisation et des ressources dont elle dispose, ce plan fera également appel à des services externes tels que des services informatiques externalisés, des ressources humaines (RH) et du personnel de sécurité. Chaque organisation doit tenir compte de sa situation particulière lors de l'élaboration de son plan d'intervention immédiate.

Chaque rôle et responsabilité inclus dans le PAU doit être clairement défini et délégué à des personnes ou des équipes spécifiques parmi les employés de l'organisation. En l'absence de rôles clairement définis, de nombreux employés seront peu susceptibles ou incapables de prendre les mesures qui s'imposent en cas d'urgence. Il faut tenir compte des horaires variables des employés, de leur accès aux différents étages ou zones de l'installation et de leur maîtrise de l'anglais écrit et parlé lorsqu'ils se voient confier ces rôles. Le cas échéant, faites participer le ou les syndicats de l'organisation dès le début du processus de planification d'urgence ; il ou ils pourraient être utiles pour établir les plans spécifiques à l'installation, attribuer les rôles et veiller à ce que toutes les préoccupations des employés soient prises en compte[3].

---

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

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.

Lors de l'élaboration du PAU, les dirigeants de l'organisation, ainsi que son directeur de la sécurité (ou toute fonction équivalente qui traitera directement avec les forces de l'ordre et les premiers intervenants) doivent être formés au système national de gestion des incidents (National Incident Management System [NIMS])[4]. Parmi les autres outils fédéraux destinés à aider les organisations à élaborer des plans complets et personnalisés de lutte contre la violence, citons la boîte à outils du bureau pour les services aux victimes d'actes criminels (Office for Victims of Crime)[5], le guide de préparation de l'Agence fédérale de gestion des situations d'urgence (Federal Emergency Management Agency [FEMA])[6] et l'outil électronique PAU de l'Administration de la sécurité et de la santé au travail (Occupational Safety and Health Administration [OSHA])[7]. Les dirigeants d'une organisation doivent connaître et maîtriser l'ensemble de ces ressources. Ils doivent consulter régulièrement ces ressources (p. ex. une fois par an) pour se rafraîchir la mémoire et s'assurer que leurs informations sont à jour.

Immédiatement après un incident impliquant un assaillant actif, le PAU doit lancer les procédures ci-dessous. Ces procédures doivent être désignées, développées et exercées bien avant l'incident.

Système de notification

La réponse à un incident impliquant un assaillant actif doit commencer par la notification. Le PAU doit mettre en place un système permettant de notifier un incident à l'ensemble du personnel présent sur le site, et notamment de lui conseiller d'évacuer ou de se mettre à l'abri[8]. La ou les personnes responsables du déclenchement de ce système de notification doivent être désignées à l'avance. L'organisation peut inclure des messages préétablis qui doivent pouvoir être adaptés à la situation.

Le cas échéant, coordonner avec le ou les syndicats de l'organisation pour s'assurer que ce système de notification peut être reçu et compris par tous les employés, y compris ceux qui ont des barrières linguistiques ou des besoins d'accès et fonctionnels, ainsi que ceux qui se trouvent dans des zones bruyantes, isolées ou fermées de l'installation. Une notification doit également être envoyée aux employés qui ne sont pas sur le site (p. ex. les travailleurs qui se trouvent dans un autre bâtiment, ceux qui ne viennent pas travailler ce jour-là ou ceux qui effectuent un travail hors site) pour les informer qu'ils doivent éviter le site en raison d'un incident en cours.

Cheminements d'évacuation

La direction d'une organisation (p. ex. les responsables ateliers, les cadres ou les superviseurs, en fonction du bâtiment en question et de la connaissance qu'ont les employés de son agencement) doit établir les cheminements d'évacuation avant l'incident et s'assurer que tous les employés les connaissent. Les cheminements doivent être physiquement accessibles aux occupants ayant des besoins fonctionnels et d'accès. Cela concerne, en plus du personnel présent, tous les visiteurs potentiels du site. L'organisation doit afficher un plan d'évacuation indiquant ces cheminements d'évacuation dans l'ensemble de ses bâtiments et en conserver une copie dans le PAU. Cette copie sera mise à jour au besoin.

Ce plan doit comprendre au moins deux cheminements d'évacuation et faire l'objet d'un exercice régulier (p. ex. une fois par an) par les employés afin de tenir compte des itinéraires de fuite qui pourraient être bloqués, des dangers, des voies d'accès coupées ou d'autres obstacles susceptibles d'apparaître pendant ou immédiatement après un incident impliquant un assaillant actif. En fonction de la nature de l'attaque, les itinéraires empruntés lors des exercices d'entraînement d'évacuation en cas d'incendie peuvent ne pas être sûrs voire impossibles à suivre. Les sorties non traditionnelles, comme les fenêtres et les toits, peuvent être utilisées comme voies d'évacuation si nécessaire. S'assurer que les employés puissent y accéder (clés, outils pour briser les vitres, etc.).

Les voies d'évacuation des manufacturiers essentiels dépendent de l'emplacement et de l'agencement du bâtiment, ainsi que de la nature des opérations de fabrication. Les organisations doivent répondre à un certain nombre de questions lorsqu'elles planifient les itinéraires d'évacuation :

- Les employés travaillent-ils dans un bureau ou dans un atelier de fabrication ?
- L'entreprise dispose-t-elle d'un site unique ou les employés sont-ils répartis sur plusieurs sites ?

---

4 FEMA, "National Incident Management System," consulté le 13 juillet 2023, https://www.fema.gov/emergency-managers/nims.

5 Office for Victims of Crime Training and Technical Assistance Center, "Mass Violence and Terrorism," consulté le 13 juillet 2023, https://www.ovcttac.gov/massviolence/?nm=sfa&ns=mvt&nt=hvmv.

6 FEMA, *Are You Ready?* mis à jour en avril 2023, https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf.

7 Occupational Safety and Health Administration (OSHA), "Emergency Action Plan," consulté le 13 juillet 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*, septembre 2021, https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf.

- Le bâtiment dispose-t-il d'un système de sécurité dont il faut tenir compte ?
- Y a-t-il des machines qui doivent être arrêtées avant l'évacuation ?
    - Si les machines doivent être arrêtées ou mises hors service avant l'évacuation, il faut s'assurer que les employés (les ouvriers, les chefs d'atelier ou toutes autres personnes concernées, en fonction de la structure de l'organisation) sont en mesure de le faire rapidement, efficacement et sans craindre de répercussions en cas d'interruption des opérations. Toutefois, il faut veiller à ce que les employés comprennent que leur sécurité est la priorité absolue de l'organisation ; si l'équipement de fabrication ne peut pas être désactivé à temps, ils doivent se diriger vers la voie d'évacuation le plus rapidement possible.

Si une organisation ne sait pas comment planifier les itinéraires d'évacuation de son bâtiment, elle peut prendre contact avec les forces de l'ordre locales, qui pourront peut-être se rendre sur place et l'aider à planifier les meilleurs itinéraires.

Outre l'établissement d'itinéraires d'évacuation, il convient de s'assurer que les employés connaissent les bonnes pratiques suivantes en matière d'évacuation :

- Il faut laisser ses effets personnels derrière soi.
- Il faut sortir en levant les mains en l'air pour signaler aux forces de l'ordre qu'on n'est pas armé.
- Il faut éviter les escaliers roulants et les ascenseurs.
- Il est bien d'emmener d'autres personnes avec soi, mais il ne faut pas rester en arrière parce que d'autres refusent de partir.
- Appeler le 9-1-1 dès qu'il est possible de le faire en toute sécurité.

Lorsque vous appelez le 9-1-1, fournissez autant d'informations que possible aux répartiteurs :

- *Lieu de l'incident, y compris l'adresse, le numéro du bâtiment, l'étage et toute autre information nécessaire (p. ex. salle 123, zone de chargement 4) ;*
- *Lieu où se trouve la personne qui appelle ;*
- *Lieu où se trouve l'assaillant actif (et s'il y en a plus d'un, combien sont-ils ?) ;*
- *S'il y a du personnel chargé de l'application de la loi ou de la sécurité sur le site, le cas échéant ;*
- *Description physique de l'agresseur ou des agresseurs, le cas échéant ;*
- *Type et nombre d'armes utilisées par le ou les assaillants, le cas échéant ;*
- *Utilisation ou menace d'utilisation d'explosifs ou menace d'engins explosifs improvisés (EEI) ;*
- *Si l'attaque est toujours en cours ; et*
- *le nombre de victimes potentielles sur les lieux.*

Lorsque l'évacuation n'est pas possible en raison de l'emplacement du ou des assaillants ou des dommages faits, les employés doivent connaître les lieux de mise à l'abri au sein de l'installation – ceux-ci doivent idéalement être dotés d'une porte verrouillable et d'autant de cachettes et d'abris que possible. Les employés réfugiés dans un lieu de mise à l'abri de l'installation doivent rester où ils sont jusqu'à ce que les services d'urgence les informent qu'ils peuvent se déplacer en toute sécurité.

Équipes d'évacuation

Lors d'une évacuation, l'objectif le plus important est que les employés sortent le plus rapidement possible. Dans la pratique, cela signifie que de nombreuses personnes peuvent sortir du ou des bâtiments par plusieurs issues, ce qui complique le rassemblement après une évacuation et le comptage des employés manquants. Le PAU doit désigner un certain nombre de salariés (p. ex. les responsables atelier, de l'installation ou de zone) qui suivront une formation d'équipiers d'évacuation dont la responsabilité sera de faire le pointage du personnel après une évacuation pour s'assurer que personne ne manque. Les équipiers d'évacuation permettent à une organisation de déterminer l'état et la localisation du personnel ; leur rôle est aussi d'aider les forces de l'ordre et les services médicaux d'urgence et au besoin de notifier les familles.

Le PAU doit informer toutes les personnes évacuées qu'elles doivent, si possible, se mettre à l'abri dans des lieux fermés proches (comme des bureaux, hôtels ou centres de conférence), afin de pouvoir faire face aux intempéries. Il doit également indiquer aux employés d'éviter de s'attarder dans les parkings attenants à l'entreprise, car les assaillants peuvent avoir laissé des engins explosifs improvisés dans les véhicules.

Dans la mesure du possible, choisir un lieu suffisamment spacieux pour accueillir l'ensemble du personnel sur place, ainsi que des espaces spécifiques (salles, tentes ou bâtiments adjacents) que l'équipe d'évacuation peut réserver pour les services d'urgence, la police, les médias, les familles et les proches, ainsi que pour les personnes nécessitant des soins médicaux. Notamment, les médias et la presse doivent être dirigés vers un lieu spécifique et séparé afin de les tenir à l'écart des familles et des employés touchés et de ne pas gêner les services d'urgence. L'équipe d'évacuation doit également prendre en compte les besoins potentiels de l'ensemble du personnel une fois évacué, y compris l'accessibilité physique au lieu où ils se trouvent et l'accès aux ressources dans d'autres langues.

Les équipiers d'évacuation répertorient tous les membres du personnel comptabilisés, manquants ou blessés, et tiennent la liste à jour en fonction de l'évolution de la situation. Ces équipiers doivent être informés, à l'avance, des employés travaillant hors site ou absents de l'organisation, ainsi que de ceux présents sur le site (p. ex. les employés, les clients, les sous-traitants et les fournisseurs). Cependant, il peut être difficile d'obtenir un comptage précis ou tout simplement de compter les personnes évacuées car celles-ci peuvent être dans l'impossibilité de se rassembler en un seul endroit et certains membres du personnel n'ont pas pu évacuer les lieux et se trouvent encore à l'abri à l'intérieur du ou des bâtiments. C'est pourquoi le PAU peut envisager l'utilisation d'outils dits de responsabilité tels qu'une application de pointage (check-in).

L'équipe d'évacuation partagera également ces informations avec les services d'urgence afin de faciliter l'aide médicale et les retrouvailles avec les familles et les personnes à contacter en cas d'urgence. Si des mineurs figurent parmi les personnes évacuées, les organisateurs doivent veiller à identifier correctement leurs parents ou tuteurs afin de s'assurer de leur bien-être.

Le fait de prendre ces mesures pour déterminer à l'avance quelles sont les responsabilités de chacun encouragera les discussions lors de l'élaboration du PAU afin d'identifier et de planifier les efforts d'intervention connexes, tels que la coordination de ressources suffisantes (p. ex. nourriture, boissons, thérapeutes, membres du clergé) dont les personnes évacuées et les intervenants peuvent avoir besoin.

Équipes d'intervention médicale

L'équipe d'intervention médicale est composée de personnes clairement désignées pour répondre aux besoins immédiats et assurer la sécurité physique après le sauvetage (p. ex. premiers soins immédiats, RCP, premiers soins différés, morgue). Certaines grandes entreprises disposent peut-être déjà d'équipe d'intervention médicale, mais la plupart des petites et moyennes entreprises devront confier ces rôles à leurs employés dans le cadre de leur plan de gestion des urgences.

Dans la mesure du possible, l'équipe d'intervention médicale doit comprendre du personnel formé aux premiers secours et à la réanimation cardio-pulmonaire. Cela peut obliger l'entreprise à dispenser une formation aux premiers secours ou à exiger un certificat de réanimation cardio-pulmonaire pour une partie ou la totalité de ses employés. Les ressources existantes peuvent aider les entreprises et leurs employés à comprendre ce qu'ils doivent savoir et peuvent leur enseigner les premiers secours de base, accessibles, ainsi que quand l'utiliser et comment le coordonner avec les services d'urgence ; ces ressources comprennent l'initiative Stop The Bleed®[9] du American College of Surgeons et le You Are the Help Until Help Arrives (vous êtes les secours jusqu'à ce que les secours arrivent) de l'agence FEMA[10]. Fort de ces compétences, l'équipe d'intervention médicale a notamment pour mission d'aider les survivants et les personnes évacuées à se rendre dans les hôpitaux ou dans d'autres points de rassemblement ou vers un autre endroit. Elle apporte aussi son soutien en transportant les victimes qui ne peuvent être traitées sur place vers des établissements médicaux.

Il faut savoir qu'une bonne préparation ne se limite pas à savoir où se trouve l'hôpital le plus proche. D'autres établissements de soins peuvent être nécessaires en fonction des besoins en soins spécialisés ou d'autres facteurs (p. ex. blocage des routes à la suite de l'incident qui oblige à se diriger vers un autre lieu ou à mettre en place un plan de secours).

L'équipe d'intervention médicale doit être en mesure de fournir au personnel d'urgence et au personnel médical toutes les informations nécessaires sur l'incident afin de faciliter le traitement. Cet effort nécessite la connaissance de toutes les établissements médicaux proches et de leurs capacités ainsi que du niveau de traumatologie qu'ils peuvent traiter[11].

En fonction de leurs ressources, certaines grandes organisations peuvent disposer d'un directeur de la sécurité ou d'un autre responsable désigné qui connaît déjà les établissements médicaux de la région et leurs capacités, et qui a établi des relations avec ces établissements et avec les forces de l'ordre nationales ou locales. Il est essentiel d'entretenir des relations avec ces établissements pour assurer une communication efficace pendant et après un incident impliquant un assaillant actif. Les organisations qui n'ont pas de directeur de la sécurité doivent veiller à ce que leur équipe d'intervention médicale tissent des liens avec ces groupes pour mieux se connaître et permettre une relation de travail positive et transparente en cas d'incident. Devant le nombre de blessés, un hôpital peut vite devenir surchargé, aussi, la capacité de communiquer le plus tôt possible avec les hôpitaux peut-elle aider les services d'urgence à se préparer et à s'organiser pour pourvoir soigner les victimes, même si l'arrivée à l'hôpital et la prise en charge des soins demeureront chaotiques[12].

---

9 Stop The Bleed®, "Get Trained!", consulté le 12 juillet 2023, https://www.stopthebleed.org/training/.

10 Federal Emergency Management Agency (FEMA), "You Are the Help Until Help Arrives," consulté le 12 juillet 2023, https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US.

11 Health Resources and Services Administration, "Find a Health Center," consulté le 13 juillet 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.

Groupes de sécurité de l'infrastructure

Selon les motivations et les méthodes de l'assaillant, des dommages considérables peuvent être causés aux actifs cybernétiques et physiques d'une organisation, y compris l'équipement de fabrication, les ordinateurs et les systèmes en ligne, les systèmes de sécurité et les produits manufacturés. Des groupes de sécurité de l'infrastructure doivent être mis en place pour assurer la sécurité cybernétique et physique de ces actifs et diminuer le risque de vol ou de compromission des données à la suite d'un incident.

Les grands manufacturiers essentiels peuvent avoir du personnel ou des bureaux dédiés à la sécurité physique et la cybersécurité qui fonctionnent comme des groupes de sécurité de l'infrastructure. Toutefois, les petites et moyennes entreprises devront probablement établir leur propre groupe. En fonction de la taille, de la configuration et des ressources de l'organisation, sa sécurité physique et cybernétique peut être gérée par une entreprise tierce (p. ex. un fournisseur informatique externe peut fournir des services de cybersécurité à l'entreprise). Si c'est le cas, ces entreprises tierces doivent être alertées dès que possible en cas d'incident impliquant un assaillant actif et être tenues au courant afin de prévenir les brèches de cybersécurité ou le vol de données. L'organisation doit prévoir un moyen de communication de secours pour joindre cette entreprise en cas de panne de courant ou d'arrêt des systèmes (p. ex. e-mail, téléphone portable, téléphone fixe).

Plus précisément, les groupes de sécurité de l'infrastructure doivent être gérés par le service informatique (en interne ou externalisé, selon la structure de l'organisation) et par une équipe de sécurité physique, dirigée par un directeur de la sécurité physique. Cette personne est le chef de file de l'organisation pour tout ce qui concerne les questions de sécurité physique et, en collaboration avec le service informatique, elle fournit un soutien et un leadership unifiés en matière de gestion des risques de sécurité dans l'ensemble de l'organisation. Si certains manufacturiers essentiels disposent d'une équipe et d'un directeur de la sécurité physique, ce n'est pas le cas pour d'autres, en particulier ceux qui disposent de moins de ressources, d'installations plus petites ou de niveaux de sécurité inférieurs. Ces organisations devront attribuer elles-mêmes ces responsabilités, que ce soit à des employés de l'organisation (p. ex. des superviseurs, des responsables atelier ou tout autre personnel responsable et compétent) ou au responsable de la sécurité du bâtiment, de l'installation ou du complexe de l'organisation. Le personnel de la technologie de l'information et le personnel chargé de la sécurité physique doivent communiquer de manière transparente entre eux et avec le reste de l'organisation.

Les incidents impliquant des agresseurs actifs sont effrayants et inattendus, de ce fait, les gens hésitent souvent à agir face à une menace, surtout s'ils sont les premiers de leur site à mettre en place des protocoles d'urgence. Plus une organisation et son personnel connaissent leur plan de gestion des urgences, plus ils seront confiants dans sa mise en œuvre et plus ils seront disposés et capables d'aider les autres personnes présentes sur le site (que les autres employés ou visiteurs ignorent ou non le plan de gestion des urgences de l'organisation).

Pour être efficaces, ces mesures d'intervention immédiate doivent inclure tous les échelons des salariés ainsi que plusieurs équipes constituées avant l'incident, dont beaucoup resteront actives au-delà des efforts d'intervention de l'organisation et jusqu'à sa récupération à court et à long terme. Outre les mesures de gestion des urgences susmentionnées, l'organisation doit définir les responsabilités suivantes.

RESPONSABILITÉS DE L'ÉQUIPE DE COMMUNICATION

Une communication précise et rapide au cours de l'intervention est essentielle pour qu'une organisation reçoive une aide adéquate de la part des services d'urgence et des forces de l'ordre. La communication est également utilisée pour fournir des informations précieuses et pratiques, non seulement sur ce qu'on sait sur l'incident mais aussi sur les fermetures de routes ou les ressources disponibles pour les personnes directement concernées pas l'incident. De plus, il faut prendre contact avec les membres de la famille des employés et les tenir informés. Les organisations doivent veiller à ce que leur communication durant cette période difficile soit exacte, cohérente et utile à toutes les personnes concernées, notamment en assumant les responsabilités suivantes :

- Les personnes désignées par le PAU, ainsi que le personnel de sécurité sur place, doivent communiquer avec les services d'urgence et les forces de l'ordre.
- Les RH, qu'elles soient internes ou externalisées, doivent tenir les employés et leurs familles informés.
- Les cadres dirigeants de l'organisation, l'équipe juridique (interne ou externalisée), l'équipe des affaires extérieures (s'il y en a une) et les employés assignés à une équipe de communication de crise doivent communiquer avec les médias.

Bien que chaque moyen de communication soit différent, tous les efforts de communication doivent être coordonnés dans leur ensemble.

Intervention d'urgence

Le personnel de sécurité, ou un employé désigné, de l'organisation doit se coordonner avec les services d'urgence et les forces de l'ordre afin de garantir une intervention adéquate en cas d'urgence. Le personnel de sécurité doit établir un plan de communication prédéterminé à l'intention de tous les acteurs susceptibles d'intervenir en cas d'agression active (p. ex. les forces de l'ordre, les services d'urgence). Le personnel de sécurité doit également être prêt à communiquer avec les porte-parole de la police et des services d'urgence dès leur arrivée et à les aider à intégrer les procédures de l'organisation le plus rapidement possible (p. ex. où ils doivent se trouver, où ils peuvent traiter les victimes, les itinéraires préétablis pour l'arrivée et la sortie).

Ce personnel doit collaborer avec les forces de l'ordre et le personnel médical pour identifier les employés qui ne sont ni présents au point de rassemblement ni dans les hôpitaux ni à la morgue. Ce personnel doit être en mesure de confirmer si des employés étaient ce jour-là, absents, en voyage, travaillaient à domicile ou dans une autre installation, etc. Il doit également tenir compte des personnes présentes dans le bâtiment mais ne faisant pas partie des employées, comme les invités, les clients, les fournisseurs, les équipes d'entretien, les livreurs, etc.

Facilitation de l'information

À la suite d'un incident, différentes informations doivent être communiquées – et de différentes manières – aux employés et à leurs familles, ainsi qu'aux médias et aux forces de l'ordre. Diffuser les bonnes informations aux canaux appropriés peut s'avérer une tâche ardue et nécessitera une coordination à l'échelle de l'organisation.

Les organisations doivent envisager d'utiliser une technologie de communication de masse pour pouvoir envoyer des alertes et des mises à jour à l'ensemble du personnel afin que les employés puissent prendre des mesures immédiates. Ce système doit être mis en place et pratiqué avant un incident, avec des personnes autorisées spécifiques responsables de l'envoi de ces notifications. Les personnes chargées de cette communication doivent créer des messages prérédigés qui peuvent être adaptés et envoyés rapidement en cas d'urgence. Ces personnes doivent également configurer ces alertes pour qu'elles soient envoyées sur plusieurs canaux (p. ex. par téléphone portable et par e-mail) au cas où certaines méthodes de communication seraient temporairement indisponibles.

Au-delà de la communication à l'échelle de l'organisation, le personnel des ressources humaines doit communiquer des informations pratiques aux employés et à leurs familles, telles que les faits connus concernant l'incident, les fermetures de routes, le dénouement de l'incident et l'état des installations, ainsi que les notifications d'assistance et de responsabilité appropriées. Si une organisation n'a pas de personnel des ressources humaines attitré, cette responsabilité peut incomber à la direction de l'installation ou de l'entreprise, en fonction de la structure de l'organisation. Là encore, les personnes responsables doivent être prêtes à utiliser plusieurs canaux de communication si nécessaire. Avant l'incident, les ressources humaines doivent créer et tenir à jour une liste de contrôle des informations nécessaires et appropriées à distribuer et à annoncer au personnel et aux familles ; cette liste, tout comme les messages prérédigés de l'organisation, doit être mise à jour en conséquence à la suite de l'incident.

Les forces de l'ordre sont généralement chargées d'annoncer les décès, mais toutes les organisations concernées doivent connaître leurs responsabilités et savoir comment transmettre les informations avec précision et compassion. Le personnel doit être prêt à informer directement les membres de la famille de l'incident, y compris éventuellement faire part des employés manquants, blessés ou décédés[13]. Les informations concernant les employés manquants, blessés ou décédés ou les nouvelles sensibles de ce type doivent être communiquées dans un lieu clos et privé (p. ex. dans une pièce séparée du point de rassemblement de l'organisation, si possible). Une organisation peut être tenue de contacter les médecins légistes ou les aumôniers en cas de décès d'un employé.

Comme indiqué, le personnel des ressources humaines est chargé de faciliter l'obtention d'informations précises et opportunes concernant un incident. Toutefois, la désinformation peut constituer un obstacle à un partage efficace de l'information. La désinformation peut se propager rapidement et les rumeurs peuvent s'opposer aux faits. Le personnel des ressources humaines doit disposer d'un plan indiquant quand et comment il compte contrôler les rumeurs qui sapent les efforts déployés par l'organisation après l'incident. Il peut s'agir d'écrire une déclaration qui résumera la rumeur et la démentira.

---

13 FBI, *Developing Emergency Operations Plans: A Guide for Businesses*, mars 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*, mai 2021, https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide.

Médias

Les organisations doivent créer une équipe de communication de crise chargée de coordonner les relations avec les médias. Cette équipe doit comprendre des cadres dirigeants ainsi que l'équipe juridique de l'organisation et le service des affaires extérieures, le cas échéant. Cette équipe élaborera et communiquera des informations sur l'incident aux médias, au personnel chargé de l'incident et à d'autres organisations, le cas échéant. Des contacts et des relations de travail doivent être établis avec les médias locaux avant l'incident. En outre, la personne ou l'équipe doit élaborer à l'avance des points de discussion standards que les dirigeants de l'organisation doivent utiliser lorsqu'ils s'adressent aux médias, en utilisant un langage uniforme et clair. Le personnel juridique et le personnel chargé des affaires extérieures doivent travailler ensemble pour s'assurer que rien n'est dit qui pourrait causer des problèmes à l'entreprise.

Selon la taille et les ressources de l'organisation, il peut s'agir d'une équipe de communication interne ou d'un tiers. Quoi qu'il en soit, cette personne ou cette équipe doit avoir un lien direct avec les dirigeants de l'organisation. Les entreprises peuvent décider d'engager ou de faire appel à une société de gestion de crise spécialisée dans le traitement des incidents en matière de questions juridiques et de communication.

RESPONSABILITÉS DU SERVICE INFORMATIQUE

Une approche plus proactive des procédures d'intervention minimise la confusion et les erreurs de jugement pendant et immédiatement après un incident. Selon la gravité de l'incident, les antennes-relais de téléphonie mobile locales peuvent être submergées par le volume d'appels, ce qui limite les communications. Pour cette raison, il peut être nécessaire d'utiliser temporairement différents canaux, par exemple en publiant des mises à jour sur le site web ou les pages des médias sociaux de l'organisation, ou en utilisant des lignes d'information automatisées pour informer les appelants de la situation. Les professionnels de l'informatique de l'organisation (qu'ils appartiennent au service informatique de cette dernière ou que l'organisation fasse appel à un service tiers) doivent prévoir d'utiliser ces canaux de communication et se préparer à les adapter si nécessaire pendant l'intervention en cours.

Les personnes qui gèrent les canaux de communication de l'entreprise doivent être conscientes qu'au lendemain d'un incident, l'organisation, ses employés et sa communauté peuvent être la cible de spams et de tentatives d'hameçonnage. Il peut s'agir de sites web, de messages sur les médias sociaux, de plateformes de financement participatif ou de sollicitations de spammeurs se faisant passer pour des associations caritatives. Des sous-traitants frauduleux peuvent également prendre contact avec l'organisation ou ses employés pour tenter de commettre une fraude à l'assurance[14]. Les organisations doivent effectuer des recherches approfondies avant de signer un contrat, d'engager une aide extérieure ou de faire un don, et encourager leurs employés à faire de même. La base de données des associations caritatives de l'Internal Revenue Service (IRS) des États-Unis est une ressource utile[15].

Le service informatique, en coordination avec l'équipe des affaires extérieure, les ressources humaines ou tout autre service compétent, doit avertir le personnel et le public de ces risques (p. ex. par le biais de messages sur les médias sociaux, d'un avertissement sur le site web de l'entreprise, de notifications par e-mail aux employés et aux partenaires de l'entreprise).

Sensibiliser les employés aux escroqueries et fraudes potentielles :

- Les demandes de dons frauduleuses peuvent provenir de sollicitations en personne, d'appels téléphoniques, d'e-mails ou de médias sociaux.
- L'IRS tient à jour une liste des associations caritatives exonérées d'impôts. Une association caritative qui ne figure pas sur cette liste peut être frauduleuse.
- Certains noms d'associations caritatives frauduleuses peuvent ressembler de près à ceux d'associations caritatives reconnues, ou prétendre être affiliés à une association caritative existante.

Veiller à ce que les employés disposent d'un lien ou d'une liste d'associations caritatives reconnues auxquelles ils peuvent faire des dons en toute sécurité.

Réitérer aux employés la nécessité de vérifier les sites web et les adresses électroniques pour déceler toute anomalie pouvant indiquer une fraude.

14 Federal Bureau of Investigation, "Charity and Disaster Fraud," consulté le 15 août 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," consulté le 18 novembre 2023, https://www.irs.gov/charities-non-profits/tax-exempt-organization-search.

DEUXIÈME PARTIE : RÉCUPÉRATION À COURT TERME

Les efforts de **récupération à court terme** d'une organisation doivent commencer une fois que les préoccupations immédiates concernant les décès, les blessures et les dommages sont passées. La récupération à court terme, qui peut s'étendre sur plusieurs jours, semaines voire sur plusieurs mois après l'incident, vise principalement à garantir la santé et la sécurité des employés de l'organisation et à assurer la reprise ou la poursuite des activités de l'entreprise.

À la suite d'un incident impliquant un assaillant actif, une organisation sera méconnaissable. Les opérations ne reprendront pas comme d'habitude une fois que les services d'urgence et les forces de l'ordre auront quitté les lieux. Selon la gravité de l'incident, il se peut que les opérations ne reprennent pas – partiellement ou totalement –, pendant des semaines, voire des mois. En outre, traiter les traumatismes physiques et mentaux nécessitera beaucoup d'efforts. Une organisation doit être consciente que, quelle que soit la manière dont elle répond aux besoins des employés après un incident, ceux-ci peuvent toujours être réticents ou incapables de reprendre le travail.

Pour aider une organisation et ses employés à se remettre sur pied, il faudra faire appel à un grand nombre d'équipes et de processus créés au cours de la phase d'intervention immédiate, ainsi qu'à de nouvelles équipes et à des efforts entrepris par d'autres membres de l'organisation.

RESPONSABILITÉS DES CADRES DIRIGEANTS

Les responsabilités des cadres dirigeants vont bien au-delà de la réponse initiale de leur organisation et s'étendent aux efforts de récupération à court et à long terme. Dans les jours et les semaines qui suivent un incident, les employés sont confrontés à des bouleversements importants dans leur vie personnelle et professionnelle. Il est essentiel que l'équipe dirigeante joue un rôle actif dans les premières étapes pour remettre sur pied l'entreprise.

Les cadres dirigeants jouent un rôle essentiel dans la reprise après un tel sinistre et dans la continuité d'activité. Ils doivent prendre des mesures proactives, se coordonner étroitement entre eux et avec le reste de l'organisation ; ils doivent également donner la priorité non seulement à la continuité d'activité, mais aussi à la sécurité et à la santé de leurs employés. En outre, les cadres dirigeants sont chargés de guider efficacement les différents services qu'ils supervisent afin de minimiser les dommages à court et à long terme causés à l'organisation lorsqu'une crise survient. Toutes les décisions relatives à l'information et à la communication concernant l'incident doivent être prises par le chef de l'équipe de crise ou de l'incident.

Les cadres dirigeants devront également superviser la restitution des effets personnels des employés laissés sur place au cours du processus d'évacuation. Ils doivent informer tous les membres du personnel que leurs effets personnels ne peuvent être récupérés tant que l'enquête sur le lieu de l'incident n'est pas terminée. En coordination avec les forces de l'ordre, les cadres dirigeants doivent établir un point central de collecte des effets personnels et veiller à ce que ces objets (dont beaucoup peuvent être coûteux et faire l'objet de vols, comme les téléphones portables, les portefeuilles et les ordinateurs) soient stockés et gardés de manière sécurisée.

RESPONSABILITÉS DE L'ÉQUIPE DE COMMUNICATION

Comme pour le cadre dirigeant, les responsabilités de l'équipe de communication s'étendent au-delà de la phase de réponse immédiate à la crise et s'étendent à la récupération à court terme. Cette équipe doit continuer à superviser les mises à jour nécessaires du site web de l'organisation ou des canaux des différents médias sociaux pour s'assurer que les clients, les organisations partenaires et les proches des employés sont informés en ce qui concerne les inquiétudes en matière de sécurité et de continuité d'activité[16].

L'équipe de communication doit établir une stratégie de communication qui fournit des informations précises et opportunes tout au long des premières étapes du processus de récupération à court terme. Toutes les organisations ne sont pas suffisamment robustes pour disposer d'une équipe complète de gestion de crise ou d'incident. Il convient donc de nommer au moins une personne chargée de superviser les responsabilités en matière de communication post-incident. L'individu ou l'équipe de communication doit se coordonner avec les cadres dirigeants et le cadre dirigeant pour distribuer de manière appropriée le contenu et les mises à jour qui soulignent les efforts proactifs de l'organisation pour gérer l'incident tout en maintenant l'image publique de l'organisation et le plan de continuité d'activité.

16 DHS, ready.gov, "Crisis Communications Plan," consulté le 13 juillet 2023, https://www.ready.gov/crisis-communications-plan.

L'équipe de communication doit également veiller à ce que les familles des victimes n'apprennent pas l'incident par des canaux publics avant d'en être informées en privé par l'organisation. En outre, l'organisation peut envisager de mettre en place une ligne d'assistance téléphonique que les employés et leurs proches peuvent appeler pour recevoir des mises à jour et accéder à des ressources pertinentes.

RESPONSABILITÉS DU SERVICE INFORMATIQUE

Le service informatique de l'organisation devra déterminer si les principaux équipements informatiques ou de télécommunications de l'installation ont été endommagés ou mis hors service au cours de l'incident. La réparation de ces équipements et leur remise en service peuvent prendre des jours, voire des semaines. Toutefois, les organisations peuvent s'assurer que cet aspect de la récupération à court terme se déroule de la manière la plus harmonieuse et la plus efficace possible en mettant en œuvre des mesures approfondies de préparation aux risques (comme des systèmes redondants, des fichiers de récupération hors site, etc.) bien avant que le processus de récupération ne soit nécessaire.

La fonction première du service informatique d'une organisation est de coordonner et de fournir le contexte et les informations relatives aux impacts informatiques liés à l'événement initial ou aux actions de rétablissement à court terme. Les services informatiques doivent procéder à une évaluation des risques peu de temps après un incident, y compris une caractérisation complète du système, l'identification des menaces et des vulnérabilités, une analyse du contrôle et de l'impact ainsi qu'une détermination immédiate des risques pour les mesures d'atténuation de la reprise à court terme.

RESPONSABILITÉS JURIDIQUES

À la suite d'un incident impliquant un assaillant actif, une équipe doit être mise en place pour gérer les responsabilités juridiques de l'organisation. Cette équipe devrait être composée de l'équipe juridique existante de l'organisation (sur place ou sous contrat) qui supervise les questions juridiques pour l'organisation. Pour gérer correctement tout litige éventuel, l'organisation peut également avoir besoin d'établir des partenariats ou des liens avec des agences ou des organisations juridiques externes avant qu'un incident ne se produise.

Un incident impliquant un agresseur actif est susceptible de donner lieu à des poursuites, qu'elles soient civiles (p. ex. pour négligence ou décès injustifié) ou pénales. Cette équipe doit être préparée à parler au nom de l'organisation pendant le procès, ce qui implique d'être capable de décrire avec précision l'incident et ses conséquences, de comprendre ce qui peut être révélé publiquement et ce qui doit rester privé, et de gérer correctement l'attention des médias avant, pendant et après le procès.

Les équipes juridiques et de communication doivent se coordonner étroitement pour s'assurer que toute information transmise publiquement est légale, exacte et à jour, que la description de l'organisation elle-même est conforme à l'image de l'organisation et que la présence de l'organisation et de l'individu sur les médias sociaux reste appropriée et ne révèle pas illégalement des informations sur l'incident qui ne devraient pas être rendues publiques.

En outre, les victimes traumatisées peuvent avoir besoin d'un soutien juridique gratuit et compétent pour faire face aux responsabilités juridiques potentielles à la suite d'un incident et pendant l'enquête. L'organisation doit envisager un plan juridique préétabli pour les victimes, dans lequel les besoins juridiques des victimes sont pris en compte.

RESPONSABILITÉS EN MATIÈRE DE LA CONTINUITÉ D'ACTIVITÉ

Il sera difficile, voire impossible, de poursuivre les activités de l'entreprise après un incident impliquant un assaillant actif. Les obstacles peuvent être la perte temporaire ou permanente de l'accès au lieu de travail, une réduction temporaire ou permanente de la main-d'œuvre en raison des décès, des blessures, des traumatismes ou du deuil des employés, la perte de fournitures ou les dommages causés à l'équipement ou à la technologie du lieu de travail, y compris l'équipement informatique, et la perturbation de la chaîne d'approvisionnement (à la fois en amont et en aval). L'installation restera une scène de crime faisant l'objet d'une enquête, potentiellement pendant une période prolongée ; les dirigeants de l'organisation doivent s'attendre à ce que ces perturbations soient de la même ampleur et planifier en conséquence.

Une organisation doit établir et mettre en œuvre un plan de continuité d'activité (continuity of operations, CONOPS) bien avant qu'un incident ne se produise, afin de s'assurer que les fonctions essentielles de l'entreprise continuent après l'incident[17]. Étant donné que les employés traumatisés et blessés peuvent ne pas être en mesure de reprendre leur poste de travail pendant une longue période, voire jamais, les organisations ont besoin d'un plan pour que du personnel compétent puisse continuer à faire fonctionner l'installation, si possible.

---

17 Federal Emergency Management Agency (FEMA), Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101, septembre 2021, https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf.

Les organisations doivent élaborer et mettre en œuvre un plan de transition pour reprendre leurs activités normales aussi rapidement et harmonieusement que possible, ce qui peut inclure une transition vers un espace de travail temporaire jusqu'à ce que les bureaux ou les ateliers normalement utilisés deviennent opérationnels ou que les routes vers ou depuis l'espace de travail soient rouvertes. Du personnel compétent doit être affecté, formé et préparé à gérer le déménagement ou la réorganisation des activités, tout en tenant compte du fait que certaines installations peuvent être inaccessibles pendant que les forces de l'ordre mènent à bien leur enquête. Les organisations doivent également prévoir une redondance des communications essentielles, y compris des services informatiques, sur d'autres sites, en utilisant éventuellement les canaux de communication des parties prenantes ou d'autres organisations en amont ou en aval de la chaîne d'approvisionnement[18].

Il est essentiel de veiller à ce que ces mesures de continuité d'activité soient communiquées à l'ensemble de l'organisation, du premier au dernier échelon. Les employés à tous les niveaux de l'organisation doivent être impliqués pour s'assurer que ces procédures de récupération à court terme sont complètes et efficaces[19].

Sécurité physique du personnel, des installations et des actifs

La sécurité physique est un élément essentiel de tout plan de sécurité. La sécurité physique et la technologie physique d'une organisation jouent un rôle particulièrement important, non seulement pour protéger le personnel, mais aussi pour garantir l'efficacité et l'efficience des futurs plans de continuité d'activité. La technologie physique d'une organisation (depuis les ordinateurs et les équipements de fabrication jusqu'aux systèmes de sécurité physique existants) peut être ciblée intentionnellement par un assaillant ou endommagée ou détruite involontairement lors d'une attaque. Il est essentiel que les organisations élaborent des lignes directrices pour faire face aux dommages potentiels et planifier le remplacement ou la réparation des systèmes le plus rapidement possible afin d'assurer la continuité d'activité, de préserver leur marque et leur réputation, et d'assurer la protection de leurs employés, de leurs clients et de leurs activités.

RESPONSABILITÉS DES RH

Après un incident impliquant un assaillant actif, les employés feront face à des bouleversements importants et à une détresse, ils auront besoin de toutes les ressources à leur disposition et du soutien de leur organisation tout au long de la récupération[20]. Le service des ressources humaines d'une organisation (qu'il soit interne ou externalisé) peut jouer, ou se voir confier, de multiples rôles au cours des premières phases de la récupération à court terme, notamment :

- S'occuper des dossiers des employés décédés et des indemnités d'assurance pour les familles.
- Gérer les objets personnels des employés décédés pour les familles et veiller à ce qu'ils soient restitués de manière appropriée.
- Gérer les absences dues à des blessures ou à des traumatismes émotionnels.
- Mettre les employés en contact avec des services de santé mentale par le biais d'un programme d'aide aux employés.
- Gérer la paie, les congés maladie et les prestations médicales si les employés ne sont pas en mesure de reprendre le travail pendant une période prolongée ou s'ils ne sont jamais en mesure de reprendre le travail, etc.
- Gérer le contrôle du stress pour les employés, par exemple en offrant du temps libre aux employés qui ont supervisé les efforts de gestion de crise de l'organisation.
- Gérer les bougies commémoratives ou autres objets laissés sur le ou les lieux pour rendre hommage aux personnes décédées ou blessées. Ces éléments devront également être gérés après l'incident, et la charge ne devrait pas incomber au public.
- Envisager des associations locales à but non lucratif capables de gérer et de distribuer les dons faits par le public à la suite d'un incident.
- Les RH, l'équipe de communication et les cadres dirigeants doivent travailler ensemble pour reconnaître et répondre aux préoccupations des employés après l'incident.

---

18 CISA, Critical Manufacturing Sector Security Guide, juillet 2020, https://www.cisa.gov/sites/default/files/publications/Critical_ Manufacturing_ Sector_Security_Guide_07012020.pdf.

19 DHS, "Emergency Action Plan Guide: Active Shooter Preparedness," novembre 2017, 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," consulté le 12 juillet 2023, https://www.samhsa.gov/find-help/disaster-distress-helpline; VictimConnect, "VictimConnect Resource Center," consulté le 12 juillet 2023, https://victimconnect.org/; FBI, "FBI Victim Services," 2018, https://www.fbi.gov/file-repository/fbi-victim-services-brochure-2018.pdf/view.

TROISIÈME PARTIE : RÉCUPÉRATION À LONG TERME

La phase de **récupération à long terme** consiste en des activités qui se poursuivent bien au-delà de la période de l'incident et se concentrent sur la restauration, le redéveloppement et la revitalisation des fonctions organisationnelles et communautaires essentielles et sur le début de la gestion des efforts de stabilisation et d'atténuation. Il faut savoir que le processus de récupération complet prendra des années. La réalisation d'un bilan complet après action est essentielle pour se préparer à de futurs incidents, qu'ils soient d'origine humaine ou naturelle. Ce bilan doit être effectué en même temps que les efforts de rétablissement à long terme et peut être intégré au bilan après action et à la documentation de suivi.

Bon nombre des mesures prises dans les première et deuxième parties doivent être poursuivies à long terme, souvent en les adaptant et en les élargissant bien au-delà des structures d'équipe initiales décrites ci-dessus. Il peut également y avoir un chevauchement entre certaines activités de récupération à court terme et à long terme. Ces efforts à long terme doivent viser à garantir la santé, la sécurité et la stabilité des employés d'une organisation, ainsi qu'à soutenir la continuité d'activité, la réputation de l'organisation auprès des médias et du public, et la cybersécurité et la sécurité physique à long terme de l'organisation.

RESPONSABILITÉS EN MATIÈRE DE SANTÉ DES EMPLOYÉS

Les RH et les cadres dirigeants auront de nombreuses responsabilités à assumer au cours de la récupération à long terme de l'organisation. Il est essentiel que l'entreprise continue à prendre en charge et à répondre aux préoccupations changeantes de ses employés en matière de santé physique et mentale, dont beaucoup se prolongeront à long terme[21].

Confrontés à un traumatisme, les gens réagissent de différentes manières, souvent inattendues. Les employés peuvent être anxieux ou se sentir en danger dans certaines situations, et l'entreprise doit être prête à s'adapter à ces changements. Par exemple, les petits espaces clos (comme un bureau dont la porte est fermée) peuvent déclencher un sentiment de peur.

Il se peut que l'entreprise doive étendre ses dispositions existantes en matière de soins de santé pour garantir la santé physique et la sécurité des employés. L'entreprise peut également chercher à s'associer à des services de santé mentale externes pour répondre de manière adéquate aux besoins des employés en matière de santé mentale. Il peut s'agir d'une aide (ou counseling) au deuil pour aider les employés à faire face aux effets à long terme sur leur bien-être mental.

Outre la prise en charge des problèmes de santé physique et mentale de ses employés, l'organisation devra identifier et reconnaître les employés qui ont été blessés ou qui sont décédés. Les familles et les collègues voudront probablement commémorer l'événement d'une manière ou d'une autre sur le site des installations, soit sous la forme d'une cérémonie, soit sous la forme d'un mémorial physique, soit par les deux. Cette commémoration peut également se produire chaque année.

RESPONSABILITÉS EN MATIÈRE DE LA CONTINUITÉ D'ACTIVITÉ

Le rétablissement et le maintien des activités de l'entreprise resteront un défi dans les mois et les années qui suivront un incident[22]. Une organisation doit prendre en compte plusieurs éléments lorsqu'elle aborde les problèmes potentiels de continuité de l'activité, tels que les perturbations à long terme de la chaîne d'approvisionnement[23] ; la perte d'emploi à long terme ou permanente en raison de blessures, de traumatismes ou de problèmes de sécurité liés au retour dans les installations ; ainsi que les répercussions potentielles sur l'économie et l'image de marque de l'organisation. L'organisation doit examiner et évaluer tous les éléments de sa chaîne d'approvisionnement afin de déterminer les facteurs qui influencent sa capacité à rétablir l'approvisionnement du marché.

---

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*, août 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide.

22 DHS, *Active Shooter Recovery Guide*, août 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide.

23 CISA, *Critical Manufacturing Sector Security Guide*, juillet 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.

Comme indiqué dans la deuxième partie, une organisation sera inévitablement confrontée à une perte d'emplois à la suite d'un incident impliquant un assaillant actif et, dans de nombreux cas, cette diminution de la main-d'œuvre se prolongera sur le long terme. Les organisations doivent reconnaître que certains employés peuvent ne jamais vouloir retourner dans le même environnement ou reprendre leurs activités, même dans un endroit différent. L'impact psychologique et physique d'un tel incident traumatique est différent pour chacun. Pour maintenir au mieux les niveaux d'emploi et s'assurer que les employés actuels restent travailler dans l'entreprise, l'organisation doit comprendre et prendre en compte les diverses raisons pour lesquelles les employés ne peuvent pas ou ne veulent pas reprendre le travail. Certains employés peuvent avoir subi des blessures physiques qui dureront à long terme. D'autres peuvent encore être incapables de travailler en raison d'un traumatisme persistant, d'un deuil ou de la peur de retourner dans un environnement de travail dangereux.

Il convient de noter que les préoccupations en matière de sécurité, ainsi que la stigmatisation sociale et professionnelle qui peut apparaître au sein de l'organisation à la suite d'un incident, peuvent éloigner les employés actuels ainsi que les personnes susceptibles d'être embauchées. Pour conserver ses employés et en attirer de nouveaux, l'organisation doit se préparer à répondre à leurs besoins. Par exemple, les organisations peuvent améliorer et augmenter les systèmes de sécurité, la vidéosurveillance et les modalités de formation à la sécurité pour s'assurer que le bâtiment est sûr pour le retour de tous les employés existants et des nouveaux employés potentiels.

Les entreprises devront activement fournir et coordonner un soutien continu à tout employé souffrant d'un traumatisme existant et fournir des services de santé mentale pour répondre de manière adéquate aux besoins des employés en matière de santé mentale. Un financement supplémentaire peut être nécessaire pour mettre en place des services de counseling et de santé mentale pour les employés sur une base permanente.

En outre, les organisations devront examiner et analyser tout impact économique à long terme après l'incident afin de garantir la santé économique de l'entreprise et de préserver leur marque ainsi que leur réputation au sein de l'industrie, de la chaîne d'approvisionnement et de la communauté. L'atteinte à la réputation peut être évaluée en examinant la part de marché et le cours de l'action de l'entreprise. Dans le cadre de son analyse économique, l'entreprise devra prendre en compte les demandes d'indemnisation prolongées et d'autres types d'aide financière pour ses employés, qui peuvent s'étendre à la période de rétablissement à long terme.

RESPONSABILITÉS EN MATIÈRE DE SENSIBILISATION DU PUBLIC

Les responsabilités de l'organisation en matière de communication se poursuivront également à long terme. Les efforts de l'équipe de communication, de l'équipe juridique, des cadres dirigeants et d'autrui devront porter sur les interactions continues avec les forces de l'ordre, les services d'urgence et toute procédure judiciaire éventuelle. Ils peuvent également être chargés de tenir à jour le site web de l'organisation et sa présence sur les médias sociaux afin de transmettre des informations sur le processus de récupération. Il peut s'agir de détails sur les nouvelles mesures de sécurité, de vœux de bon rétablissement pour les personnes blessées ou des mots de condoléances pour les proches des personnes décédées lors de l'incident, et de mises à jour sur la continuité des activités. En outre, il est essentiel que l'organisation maintienne un canal de communication distinct pour les employés qui ont été directement touchés par l'incident et leurs proches. Cela permet de s'assurer qu'ils reçoivent le soutien et les informations nécessaires au cours du processus de récupération à long terme.

En outre, l'organisation devra prévoir des événements et des commémorations annuels. C'est l'occasion de réévaluer les besoins de l'organisation en matière de sécurité et de planification et de déterminer la santé, la sécurité et la stabilité des employés. Ces événements commémoratifs reconnaissent également l'impact d'un incident sur une entreprise, ses employés, leurs familles et la communauté. Ils peuvent également, selon l'ampleur de l'incident, nécessiter la coordination d'une déclaration ou d'un événement avec la presse, en plus de la publication d'une déclaration sur le site web de l'organisation et sur les pages des médias sociaux.

RESPONSABILITÉS EN MATIÈRE DE CYBERSÉCURITÉ ET DE SÉCURITÉ PHYSIQUE

Le rétablissement de la sécurité d'une organisation à la suite d'un incident – y compris la sécurité des employés et la sécurité cybernétique et physique de ses actifs – est un élément essentiel de la récupération à long terme qui peut prendre des mois, voire des années. Il existe plusieurs facteurs dont une organisation doit tenir compte dans le cadre de ses responsabilités en matière de cybersécurité et de sécurité physique. L'organisation doit analyser tous les dommages physiques et cybernétiques causés par l'incident[24], y compris les possibilités de menaces internes, les objets personnels volés ou endommagés, les systèmes de sécurité physique/cybersécurité compromis et les actifs physiques et électroniques détruits ou compromis. Cela comprend également toute atteinte ou modification de la réputation de l'organisation au sein de l'industrie, de la chaîne d'approvisionnement et de la communauté.

---

24 CISA, *Critical Manufacturing Sector Security Guide*, juillet 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.

Il est essentiel de remédier à ces dommages, non seulement pour préserver la continuité d'activité et la sécurité financière de l'organisation, mais aussi pour renforcer le sentiment de sécurité des employés au sein de l'organisation. De nombreux travailleurs ne se sentent pas en sécurité lorsqu'ils retournent sur un lieu où ils se sont sentis en danger par le passé – même après des mois ou des années – et ont besoin de voir des changements tangibles et significatifs dans les mesures de sécurité de l'organisation. L'implication des employés dans la discussion sur les améliorations nécessaires, ainsi que la sollicitation de leur avis sur ce qu'ils ont vu au cours de l'incident et qui aurait pu être évité ou atténué, peuvent constituer une étape précieuse dans la mise en œuvre de ces changements. Ces changements peuvent inclure l'installation d'un système de sécurité complet et actualisé à toutes les entrées et sorties du bâtiment, l'authentification multifactorielle pour toutes les données de l'entreprise et la formation obligatoire de tous les employés aux attaques actives, couvrant la prévention, l'atténuation et l'intervention/récupération[25]. Si l'organisation avait déjà mis en place une formation avant l'incident, une évaluation du programme peut s'avérer nécessaire pour s'assurer qu'il est à jour. La technologie évoluant très rapidement, même un nouveau programme de formation peut nécessiter une mise à jour pour tenir compte de l'évolution des menaces liées à la cybersécurité et des moyens par lesquels les systèmes de sécurité, les machines et les données peuvent être compromis.

Il faut reconnaître que pour certains employés qui ont déjà subi un traumatisme, certains programmes de formation et exercices peuvent être difficiles, voire impossibles, en raison de la détresse émotionnelle causée par le contenu de la formation. Il faut être compréhensif et compatissant envers ces employés, et chercher d'autres moyens (p. ex. des programmes de formation différents, des instructions écrites au lieu de vidéos) pour les tenir au courant des mesures de sécurité et des procédures d'urgence de l'organisation.

De nombreuses ressources fédérales existent pour informer et former les organisations et leurs employés à la détection, à la prévention et à l'atténuation des cybermenaces et des menaces physiques. Il s'agit notamment de la série de ressources [26] de la CISA sur l'atténuation des menaces internes et de leur évaluation du programme d'atténuation des risques internes (Insider Risk Mitigation Program Evaluation [IRMPE]), qui peut être utilisée pour évaluer l'état de préparation d'une organisation en cas d'incident impliquant un assaillant actif [27] . D'autres cours de formation en ligne, tels que les différents cours de préparation aux catastrophes de la FEMA, devraient être obligatoires pour les employés afin de renforcer leurs compétences en matière de préparation aux situations d'urgence[28] . Ces étapes doivent être effectuées régulièrement pour garantir la sécurité de l'organisation et la sécurité cyber-physique.

CONCLUSION

Le guide de bonnes pratiques après un incident impliquant un assaillant actif dans le secteur manufacturier essentiel sert de ressource pour les industries manufacturière essentielles, quelle que soit la taille de l'entreprise. Tous les manufacturiers essentiels et leurs filiales peuvent utiliser ce guide pour planifier leurs efforts d'intervention et de récupération après un incident.

Même si une organisation prend toutes les mesures présentées dans ce guide lorsqu'un incident se produit, il est peu probable que les employés retrouvent le niveau de confort et de sécurité qu'ils avaient avant l'incident au sein de l'organisation. De même, l'organisation peut exceller dans ses efforts de continuité d'activité et ne jamais atteindre son niveau de fonctionnement antérieur à l'incident.

Ne pas oublier que la récupération n'est pas un processus linéaire et que l'organisation touchée peut ne jamais revenir à la situation normale qui prévalait avant l'incident. Cependant, en utilisant ces étapes comme guide pour la réponse immédiate, la récupération à court terme, et la récupération à long terme, **l'organisation peut atteindre un nouveau niveau de référence pour assurer la sécurité des employés et la continuité de son activité.**

Pour plus d'informations ou pour obtenir une aide supplémentaire, prendre contact en nous écrivant à l'adresse suivante CriticalManufacturingSector@cisa.dhs.gov.

---

25 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.

26 CISA, "Insider Threat Mitigation," consulté le 13 juillet 2023, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation.

27 CISA, "Insider Risk Mitigation Program Evaluation (IRMPE)," consulté le 12 juillet 2023, https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe.

28 FEMA, Emergency Management Institute, "ISP Courses," consulté le 13 juillet 2023, https://training.fema.gov/is/crslist.aspx?lang=en.

ANNEXE A : FEUILLES DÉTACHABLES

La présente annexe fournit une série de listes de contrôle permettant aux manufacturiers essentiels et à leurs filiales de préparer leurs plans d'intervention immédiate, de récupération à court terme et de récupération à long terme à la suite d'un incident impliquant un assaillant actif. Ces listes de contrôle sont conçues pour être séparées du guide des bonnes pratiques et elles sont imprimées et distribuées selon les besoins aux cadres dirigeants, au personnel des ressources humaines et à tous les autres employés impliqués dans l'élaboration et l'exécution du plan d'action d'urgence (PAU) de l'entreprise.

Les organisations doivent adapter ces listes à leur situation et à leurs ressources spécifiques, les utiliser lors de la formation aux incidents impliquant des assaillants actifs, les garder à portée de main dans la mesure du possible lors de l'intervention et de la récupération, et les mettre à jour si nécessaire après un incident ou pour refléter tout changement dans la structure de l'entreprise ou dans le PAU.

Avant l'incident

Utilisez cette liste pour vous assurer que le PAU de l'entreprise est complet, à jour et adapté aux bâtiments, à la structure de l'emploi et au lieu où se trouve votre entreprise. Modifiez les titres et les catégories d'emploi si nécessaire et indiquez les postes qui devront être externalisés, ainsi que la ou les personnes désignées au sein de votre entreprise chargées de prendre contact et de maintenir un lien avec ces groupes externalisés avant l'incident.

Pointage immédiat au point de rassemblement

Utilisez ces listes de contrôle pour vous assurer que les employés désignés tiennent un registre précis et complet de tous les membres du personnel de l'organisation et de leur statut pendant et après une évacuation. Si nécessaire, ajoutez des lignes au tableau et incluez des colonnes distinctes pour les autres lieux spécifiques à votre PAU.

Réponse immédiate

Cette liste décrit les responsabilités de base qui incombent aux différents postes au sein d'une organisation, notamment les cadres dirigeants, le directeur de la sécurité, les ressources humaines et l'équipe juridique, afin de mener à bien un effort d'intervention immédiate rationalisé et sécurisé. Ajustez ces postes en fonction de la structure de votre organisation et adaptez les responsabilités individuelles au PAU de votre organisation.

Récupération à court terme

Comme pour les points précédents, utilisez cette liste de contrôle pour couvrir les bases du plan de récupération à court terme de votre entreprise, en ajustant les rôles et les responsabilités en fonction de la structure et de la situation de votre entreprise. Notez toutes les procédures qui devront être externalisées, ainsi que les moyens de prendre contact et de maintenir une relation de travail avec ces services et la ou les personnes au sein de votre entreprise chargées de prendre contact avec eux et de travailler avec eux après l'incident.

Récupération à long terme

Utilisez cette liste, comme les précédentes, pour définir les efforts de récupération à long terme de votre entreprise. Consultez cette liste régulièrement au cours des mois et des années de la récupération à long terme de l'entreprise, en la mettant à jour et en l'ajustant si nécessaire pour refléter tout changement de circonstances ou tout nouveau domaine d'intérêt (p. ex. le développement d'un litige, des changements dans la santé ou la situation professionnelle du personnel, des fluctuations dans la situation financière de l'entreprise).

AVANT L'INCIDENT

Directeur de la sécurité/Directeur des installations

- ☐ Élaborer et mettre en œuvre un plan d'action d'urgence (PAU). Consulter la page www.ready.gov pour des idées et des modèles, et accéder au logiciel Business Continuity Planning Suite.
- ☐ Se coordonner avec les premiers intervenants locaux (police et pompiers) pour définir une procédure de responsabilisation du personnel, des méthodes de sécurisation des zones de l'entreprise, ce à quoi il faut s'attendre pendant et après un incident, et comment et quand rendre leurs effets personnels aux employés.
  - Les sacs à main, les cartes d'identité, les ordinateurs, les téléphones, les voitures, etc., seront probablement laissés sur place lors de l'évacuation et devront être sécurisés et gardés avant d'être récupérés par les employés ou les proches.
- ☐ Coordonner les besoins de triage avec les pompiers et le personnel de première intervention. Identifier et repérer où se trouvent les centres médicaux et les centres de traumatologie de la région.
- ☐ Former le personnel aux procédures d'évacuation.
  - Veillez à ce que vos procédures d'évacuation soient pratiques pour le personnel ayant des besoins fonctionnels ou d'accès, ou qui ne parle pas couramment l'anglais.
- ☐ Créer un système de notification des employés à canaux multiples (téléphone, e-mail, etc.) et attribuer la responsabilité de son activation.
  - Effectuer des tests périodiques de ce système de notification, en veillant à ce qu'il atteigne tous les employés, quels que soient leur handicap, les barrières linguistiques ou les zones de travail très bruyantes.
- ☐ Fournir ou utiliser la formation du système national de gestion des incidents (National Incident Management System [NIMS]).
- ☐ Utiliser les ressources fédérales telles que la boîte à outils du bureau pour les services aux victimes d'actes criminels (Office for Victims of Crime), le guide de préparation de l'Agence fédérale de gestion des situations d'urgence (Federal Emergency Management Agency [FEMA]) et l'outil électronique PAU de l'Administration de la sécurité et de la santé au travail (Occupational Safety and Health Administration [OSHA]).
- ☐ Mettre en place une équipe d'évacuation et déterminer à l'avance la méthode qui sera utiliser pour le comptage du personnel (p. ex. une application de pointage [check-in]).
- ☐ Former une équipe d'intervention médicale avec des employés qualifiés pour en faire partie, si possible.
- ☐ Mettre en place, si nécessaire, un groupe de sécurité de l'infrastructure.
- ☐ Mettre en œuvre et pratiquer un plan de continuité d'activité (continuity of operations, CONOPS) complet.
- ☐ Encourager les employés à suivre une formation aux premiers secours et à la réanimation cardio-pulmonaire.
- ☐ Désigner des responsables du rassemblement pour tous les étages, toutes les installations et tous les sites afin d'assurer le suivi et de procéder au comptage.

Ressources humaines (RH)

- ☐ Travailler avec le directeur de la sécurité/des installations pour savoir où se trouvent les centres de soins et les centres de traumatologie. S'assurer que tous les points de contact (POC) sur les sites sont à jour et que les présentations ont été faites (p. ex. le personnel de communication de l'hôpital, etc.).
- ☐ Travailler avec l'équipe juridique, les affaires extérieures, le cadre dirigeant et les autres parties concernées afin d'identifier et d'organiser les points de rassemblement et les zones de relocalisation et d'obtenir les contrats nécessaires (hôtels, centres de conférence, etc.) à mettre en œuvre en cas de besoin.
  - Veiller à ce que ces parties soient tenues informées des POC en vigueur et de toute mise à jour du PAU.
- ☐ Déterminer les besoins et les prestations des employés en cas d'incidents de ce type, y compris les responsabilités de l'entreprise.
- ☐ Si un syndicat est présent dans l'établissement, travailler avec les représentants syndicaux et les employés pour identifier et traiter les questions syndicales qui doivent être prises en compte.
- ☐ Créer et tenir à jour une liste de contrôle des informations essentielles à communiquer aux employés et à leur famille en cas d'incident.

Employés

- ☐ Suivre une formation sur les assaillants actifs dispensée par l'entreprise.
- ☐ Participer aux exercices de mise en situation d'assaillants actifs organisés par l'entreprise.
- ☐ Participer aux tests du système de notification des employés et fournir un retour d'information.
- ☐ Veiller à ce que toutes les informations relatives aux POC, aux proches, etc. soient tenues à jour.
- ☐ Veiller à ce que tous les bénéficiaires de prestations médicales et d'assurance, ainsi que les autres informations, soient tenus à jour.
- ☐ Veiller à ce que les membres de la famille aient accès à des copies de toutes les informations médicales et d'assurance dans un endroit facilement accessible en cas d'urgence.

Questions juridiques

- ☐ Travailler avec le cadre dirigeant, les ressources humaines, le directeur de la sécurité et les autres parties concernées pour traiter les questions juridiques liées à des incidents potentiels.
- ☐ Travailler avec les affaires extérieures et le cadre dirigeant pour développer des points de discussion avec les médias en cas d'incident, en veillant à ce qu'aucune déclaration ne soit faite qui pourrait poser des problèmes à l'entreprise.

Affaires extérieures/communication

- ☐ Travailler avec le cadre dirigeant, les ressources humaines, le directeur de la sécurité, etc., sur les messages à envoyer aux familles et aux employés concernés et touchés.
- ☐ Rédiger des articles modèles pour les médias grand public et sociaux qui serviront aussi à la sensibilisation du public afin de faciliter la diffusion des informations. En s'y prenant à l'avance, on peut éviter que des informations erronées ne se retrouvent au premier plan dans les médias ou en ligne.
- ☐ Mettre en place une équipe de communication de crise chargée de gérer les relations avec les médias et de diffuser les informations relatives à l'incident à toutes les parties concernées, le cas échéant.
- ☐ Établir des contacts et cultiver des relations de travail avec les médias locaux.
- ☐ Travailler avec le cadre dirigeant, les RH, le directeur de la sécurité, l'équipe informatique et tout autre groupe concerné pour établir des modèles de messages pour les sites web de dons frauduleux potentiels, les sollicitations, etc. Se préparer à lutter contre les activités frauduleuses en publiant ou en annonçant régulièrement des informations exactes sur les donateurs.

Équipe informatique/réseau

- ☐ Collaborer avec le directeur de la sécurité pour préserver la cybersécurité et les actifs cybernétiques de l'entreprise en cas d'incidents physiques.
- ☐ Maintenir en permanence l'intégrité du réseau.
- ☐ Si nécessaire, aider à la mise en place d'un système de notification des employés.
- ☐ Prévoir d'utiliser d'autres canaux de communication, tels que les médias sociaux et les sites web de l'entreprise, et se préparer à les adapter si nécessaire au cours de la réponse à l'incident.
- ☐ Établir des plans dans lesquels les auteurs potentiels de la menace pourraient tirer parti d'un système de réseau dégradé au cours d'un incident.

Finance/sous-traitants/fournisseurs

- ☐ Incorporer des clauses contractuelles concernant les incidents d'origine humaine.
- ☐ Assurer le suivi avec les fournisseurs et les clients pour évaluer les achats ou les commandes en cours.

POINTAGE IMMÉDIAT AU POINT DE RASSEMBLEMENT

- **Noter et trier les personnes blessées pour les secours médicaux d'urgence.**
- **Le cas échéant, utiliser des méthodes préétablies pour transporter les employés en lieu sûr.**

À la suite d'une évacuation, les membres du groupe d'évacuation désigné doivent procéder à la comptabilité du personnel, notamment le nombre total de personnes dans chaque catégorie ainsi que leur nom et là où elles se trouvent (si on le sait).

Équipe d'évacuation

Des responsables atelier, de l'installation ou de zone ou d'autres employés désignés préalablement comme équipiers d'évacuation auront la responsabilité de faire le pointage du personnel (y compris les blessés, les indemnes, les manquants, les personnes en voyage/en déplacement/en congé) après l'évacuation.

Recensé, hors site *(en voyage, en déplacement, en vacances, etc.)*	**Indemne**	**Manquant/on ne sait pas**	**Blessé** *(inclure hôpital ou état, le cas échéant)*
TOTAL :	TOTAL :	TOTAL :	TOTAL :

RÉPONSE IMMÉDIATE

Directeur de la sécurité/Directeur des installations

- ☐ Coordonner avec les premiers intervenants locaux.
- ☐ Veiller à ce que le cadre dirigeant, les ressources humaines, les affaires extérieures/équipe de communication sachent vers quels établissements médicaux les employés ont été emmenés.

Cadre dirigeant

- ☐ Si l'installation est encore opérationnelle, discuter du moment et quelle sera l'étendue de la reprise des activités après l'enquête.
- ☐ Prendre contact avec les employés, les familles, les clients et les actionnaires touchés par l'incident.
- ☐ Collaborer avec les affaires extérieures/équipe de communication pour assurer la couverture médiatique de l'incident.

Équipe des ressources humaines

- ☐ Collaborer avec le directeur de la sécurité/des installations pour savoir vers quels établissements médicaux les employés ont été emmenés.
- ☐ Collaborer avec l'équipe juridique, les affaires extérieures, le cadre dirigeant et les autres parties concernées pour organiser les zones de relocalisation (hôtels, centres de conférence, etc.).
- ☐ Tenir les employés et leurs familles informés de l'évolution de la situation et du lieu où se trouvent les employés.
- ☐ Mettre en place toute la documentation nécessaire pour les employés touchés qui pourraient être dans l'incapacité de travailler en raison de blessures ou pour les familles des employés décédés.
- ☐ Travailler avec les représentants syndicaux, le cas échéant, pour s'assurer que l'organisation respecte les exigences syndicales et pour aborder toute question potentielle d'ordre syndical en relation avec l'incident.
- ☐ Travailler avec des professionnels de la santé mentale pour élaborer des plans de soutien immédiat et à long terme aux victimes de traumatismes, y compris en ce qui concerne le stress post-traumatique.
- ☐ Communiquer les informations nécessaires aux employés et à leurs familles, telles que les détails confirmés de l'incident, les fermetures de routes, les mises à jour de l'état des installations (y compris la collecte des effets personnels) et les notifications d'assistance et de responsabilité appropriées.
- ☐ Informer directement les membres de la famille de l'incident de manière précise, avec compassion et en privé (cela concernera les employés potentiellement manquants, blessés ou décédés).

Équipe juridique

- ☐ Travailler avec le cadre dirigeant, les ressources humaines, le directeur de la sécurité et les autres équipes concernées afin de se préparer à toute question juridique pouvant découler de l'incident.

Équipe informatique/réseau

- ☐ Travailler avec le directeur de la sécurité pour protéger les actifs cybernétiques de l'entreprise de tout impact potentiel causé par un incident physique.
- ☐ Maintenir l'intégrité du réseau.

Équipe des affaires extérieures/de la communication

- ☐ Travailler avec le cadre dirigeant, les ressources humaines, le directeur de la sécurité et tout autre groupe concerné pour rédiger et communiquer des messages aux familles et aux employés qui ont été touchés par l'incident. Il peut s'agir d'élaborer des messages prérédigés pour faciliter la communication au lendemain d'un incident.
- ☐ Continuer à superviser la communication avec les médias jusqu'à ce que l'incident soit entièrement résolu.
- ☐ Envoyer des messages à des associations caritatives légitimes pour obtenir des dons. Conseiller aux gens de faire attention aux associations caritatives frauduleuses et de les signaler de manière appropriée.

RÉPONSE À COURT TERME

Directeur de la sécurité/Directeur des installations

- ☐ Tirer les leçons de ce qui a fonctionné et de ce qui n'a pas fonctionné en matière de sécurité.
- ☐ Intégrer les enseignements tirés de l'expérience et mettre à jour le plan d'action d'urgence (PAU) de l'organisation.

Cadre dirigeant

- ☐ Réparer tout dommage subi par les installations au cours de l'incident.
- ☐ Veiller à ce que les installations soient sûres pour que les employés puissent reprendre le travail.
- ☐ Rassurer les actionnaires en cas de baisse du marché.

Équipe des ressources humaines

- ☐ Élaborer un plan pour que le retour sur le lieu de travail des employés se fasse dans les meilleures conditions.
- ☐ Tenir compte des répercussions potentielles des traumatismes sur la capacité des employés à reprendre le travail.
- ☐ Déterminer comment traiter de manière appropriée les objets laissés dans l'établissement (faut-il les rendre aux employés, aux membres de la famille ou les utiliser dans le cadre d'une commémoration).
- ☐ Décider si l'entreprise organisera une commémoration à l'occasion de l'anniversaire de l'incident.

Équipe juridique

- ☐ Traiter les actions en justice intentées par les familles des employés blessés ou décédés.
- ☐ Gérer toute procédure judiciaire liée au(x) suspect(s).
- ☐ Se préparer à représenter l'organisation en cas de litige, notamment en décrivant avec précision l'incident et ses résultats, en gérant les déclarations publiques et en s'occupant des médias tout au long de la procédure judiciaire.
- ☐ Étudier la possibilité de mettre en place un plan de soutien juridique préétabli pour répondre aux besoins des victimes.

Équipe informatique

- ☐ Déterminer si des équipements informatiques ou de télécommunications ont été endommagés par l'incident ou ont subi des perturbations.
- ☐ Procéder à une évaluation des risques cybernétiques ou informatiques peu de temps après l'incident.

Équipe des affaires extérieures/de la communication

- ☐ Continuer à communiquer avec les employés et à répondre aux demandes des médias.
- ☐ Donner des informations précises et opportunes pendant les phases initiales de récupération à court terme.
- ☐ Coordonner avec le cadre dirigeant pour partager les mises à jour de la gestion proactive des incidents de l'équipe tout en préservant l'image publique de l'entreprise et le plan de continuité d'activité.
- ☐ Mettre en place une ligne d'assistance téléphonique que les employés et leurs proches peuvent appeler pour recevoir des mises à jour ou accéder à des ressources pertinentes.
- ☐ Travailler avec les RH pour identifier et fournir des ressources accessibles aux employés et à leurs proches en cas de besoin (médicales, psychologiques, etc.).

Équipe Finance/sous-traitants/fournisseurs

- ☐ Assurer le suivi avec les fournisseurs et les clients afin d'évaluer les répercussions sur les achats ou les commandes en cours.
- ☐ Travailler à l'obtention des coûts de récupération à court et à long terme, y compris le nettoyage et la réparation des installations, l'ajout de nouvelles mesures de sécurité fondées sur les leçons apprises, l'extension des soins de santé ou autres prestations pour les employés, etc.

RÉPONSE À LONG TERME

Directeur de la sécurité/Directeur des installations

- ☐ Intégrer les enseignements tirés dans la formation et les exercices relatifs aux incidents.
  - Mettre en œuvre de nouveaux programmes de formation sur les assaillants actifs pour les employés ou évaluer les programmes existants ; les programmes doivent être offerts et mis à jour régulièrement (p. ex. une fois par an).
- ☐ Mettre à jour le plan d'action d'urgence (PAU) existant de l'organisation.
- ☐ Mettre en œuvre de nouveaux protocoles et technologies de sécurité sur la base des enseignements tirés.
- ☐ Évaluer tous les dommages physiques après l'incident, y compris les articles volés ou endommagés, les systèmes de sécurité compromis et les actifs touchés.

Cadre dirigeant

- ☐ S'efforcer de rétablir la réputation de l'entreprise dans les médias, dans l'industrie et dans la chaîne d'approvisionnement.
- ☐ Maintenir le contact avec les employés pour les assurer de l'engagement de l'entreprise en matière de réadaptation.
- ☐ Évaluer les inquiétudes liées à la continuité d'activité, y compris les interruptions prolongées de la chaîne d'approvisionnement, les défis d'un emploi durable à cause des blessures ou des traumatismes et les répercussions économiques potentielles.

Équipe des ressources humaines

- ☐ Fournir des ressources pour un soutien à long terme en matière de santé mentale pour les employés traumatisés.
- ☐ Élargir les prestations de soins de santé des employés afin de répondre aux problèmes de santé post-incident, le cas échéant.
- ☐ Gérer et verser les indemnités d'assurance aux familles des employés décédés.
- ☐ S'adapter à l'évolution des besoins des employés en matière de santé physique et mentale.

Équipe juridique

- ☐ Traiter les actions en justice intentées par les familles des employés blessés ou décédés.
- ☐ Traiter toute action en justice liée au(x) suspect(s).

Équipe informatique

- ☐ Mettre à jour les systèmes compromis si nécessaire.
- ☐ Évaluer tous les dommages liés à la cybernétique et à la cybersécurité, y compris les systèmes compromis et la perte d'actifs électroniques.

Équipe des affaires extérieures/de la communication

- ☐ Mettre à jour le site web et les médias sociaux de l'organisation avec des mises à jour sur la récupération, les mesures de sécurité, les condoléances et les informations sur la continuité d'activité.
- ☐ Prévoir et planifier des commémorations et des événements dans les semaines, les mois et les années qui suivent l'incident, y compris éventuellement la coordination d'une déclaration ou d'un événement avec les médias, les employés et les proches des personnes décédées.

Équipe Finance/sous-traitants/fournisseurs

- ☐ Assurer le suivi avec les fournisseurs et les clients afin d'évaluer les répercussions sur les achats ou les commandes en cours (long terme).
- ☐ Travailler à la mise à jour de tous les contrats, etc., comme prévu dans le plan et intégrer les enseignements tirés de l'incident, etc.

ANNEXE B : RESSOURCES

QUE FAIRE EN CAS DE MENACE D'ASSAILLANT ACTIF

Active Shooter Emergency Action Plan Product Suite (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, Office for Bombing Prevention): 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

GUIDES POUR RÉALISER UN PLAN DE CONTINUITÉ D'ACTIVITÉ

Business Continuity Plan (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

RESSOURCES POUR UN PLAN D'ACTION D'URGENCE

Developing Emergency Operations Plans: A Guide for Businesses (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 (FEMA): https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf

Evacuation Plans and Procedures eTool (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

ASSISTANCE D'URGENCE ET AIDE AUX VICTIMES

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 (OVC): https://ovc.ojp.gov/program/antiterrorism-and-emergency-assistance-program-aeap/overview

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): 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

RESSOURCES POUR UNE PRÉPARATION PERSONNELLE

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

GUIDES DE PLANIFICATION DE LA RÉPONSE ET DE LA RÉCUPÉRATION

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/resources-tools/resources/isc-violence-federal-workplace-guide

Mass Violence and Terrorism Resources (Office for Victims of Crime & Training & Technical Assistance Center): https://www.ovcttac.gov/massviolence/?nm=sfa&ns=mvt&nt=hvmv

Workplace Violence (OSHA): https://www.osha.gov/workplace-violence/enforcement

RESSOURCES POUR LE SECTEUR DE LA SÉCURITÉ

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

FORMATION EN MATIÈRE DE SÉCURITÉ ET ÉVALUATIONS

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/crslistaspx?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