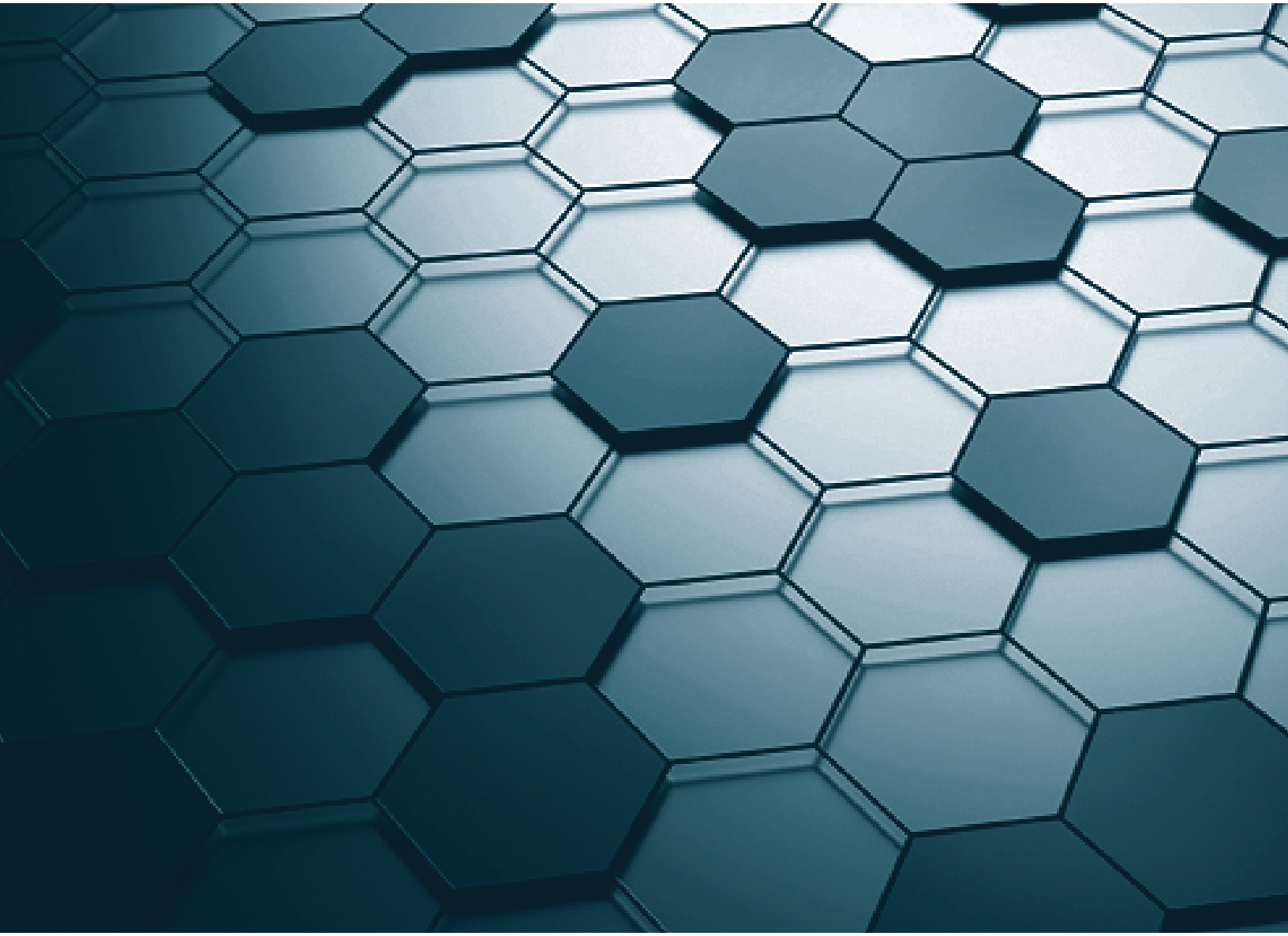
Élaboration d'un **plan d'intervention en cas d'incident de la technologie opérationnelle et de la technologie de l'information**



Sécurité publique Canada
Public Safety Canada

Canada

No de cat. : PS4-267/2020F-PDF
ISSN: 978-0-660-35444-6

Contenu

Préambule **5**

Résumé **6**

Objectif du document 7

Hypothèses 7

Comprendre un environnement de TO **8**

Déterminer les biens de TO 8

Cyberincidents 10

Évaluations des risques 11

Comprendre la structure organisationnelle **12**

Structure organisationnelle 12

Membres de l'EIIC 13

Adopter une approche centralisée ou décentralisée **15**

Approche centralisée 15

Approche décentralisée 15

La découverte par la pratique! 17

Prenez un point de vue de TO **18**

Différences entre les systèmes de réseaux de TI et de TO 18

Formation en sécurité 19

Répercussions sur la résilience 19

Élaboration d'un plan mixte d'intervention en cas de cyberincident des TI et des TO **21**

Étape 1 : Constituer une équipe interfonctionnelle 21

Étape 2 : Examiner tout plan d'intervention en cas d'incident existant au sein de l'équipe 22

Étape 3 : Définition d'un incident 24

Étape 4 : Déterminer comment les équipes vont s'assembler 27

Étape 5 : Déterminer comment les équipes communiqueront 29

Étape 6 : Déterminer les mesures d'intervention nécessaires 31

Étape 7 : Déterminer comment le PRIC s'intégrera dans un plan de gestion de crise 34

Maintenir le PRIC commun dans les TI et les TO..... 36

Conclusion 38

Glossaire 39

Préambule

La convergence des environnements des technologies de l'information (TI) et des technologies opérationnelles (TO) est une tendance croissante dans le paysage actuel de la cybersécurité, et l'élaboration de ce guide vise à informer les organisations sur la meilleure façon de répondre à cette nouvelle tendance. Les informations contenues dans ce document sont destinées à être mises à jour en permanence et seront revues et mises à jour au besoin pour répondre aux besoins évolutifs des propriétaires et des exploitants d'infrastructures critiques au Canada.

Ce document est le fruit d'une collaboration entre Sécurité publique Canada, le Centre de la sécurité des télécommunications et les membres du groupe de travail TI/TO, qui comprend les membres des organisations suivantes : Bruce Power, Cameco Corporation, ENMAX Power Corporation, Hydro Ottawa, Laboratoires Nucléaires Canadiens, Newfoundland Labrador Hydro, Mines Agnico Eagle Limitée, Pembina Pipeline Corporation, SANS Institute, SaskEnergy, SaskPower, et Société indépendante d'exploitation du réseau d'électricité (SIERE). Ce document est également approuvé par Ressources naturelles Canada (RNCan) en tant que responsable du secteur de l'énergie et des services publics pour le gouvernement du Canada. Les conseils et les orientations contenus dans ce document sont toutefois applicables à toute organisation confrontée à la convergence des environnements des TI et TO.

Résumé

Alors que de nombreuses organisations sont équipées d'outils et de ressources capables de résoudre les cyberincidents courants en matière de TI, il est de plus en plus nécessaire de traiter et d'atténuer les risques associés aux cyberincidents qui ont des conséquences sur les environnements de TO des organisations.

À mesure que la technologie devient plus intégrée et sophistiquée, il devient de plus en plus essentiel d'avoir la capacité de fournir une réponse coordonnée et efficace aux cybermenaces dans l'ensemble de l'organisation. Un plan de réponse aux incidents cybernétiques (PRIC) des TI et des TO peut garantir que l'organisation dispose des compétences et de la préparation nécessaires pour faire face aux cybermenaces qui surviennent dans tous les environnements technologiques qu'elle possède et utilise.

Les renseignements présentés dans ce document de référence visent à fournir aux organisations qui exploitent une composante des TO dans leur environnement un cadre qui peut être référencé, appliqué et mis à profit lors de l'élaboration d'un PRIC des TI et des TO adapté à leurs propres besoins opérationnels. Le document fournit une approche générale, y compris des facteurs particuliers à prendre en compte selon la taille, la fonction, l'emplacement et les considérations sectorielles de l'organisation.

Cette directive fournit des recommandations sommaires lors de la création d'un PRIC pouvant répondre aux besoins particuliers d'une organisation, des facteurs à considérer lors de la création d'une équipe d'intervention en cas des incidents cybernétiques (EIIC) correspondante, des conseils sur la manière de maintenir le PRIC d'une façon continue, ainsi que des conseils sur la manière de réfléchir aux cybermenaces courantes.

« Un plan de réponse aux incidents cybernétiques (PRIC) des TI et des TO peut garantir que l'organisation dispose des compétences et de la préparation nécessaires pour faire face aux cybermenaces qui surviennent dans tous les environnements technologiques qu'elle possède et utilise. »

Objectif du document

L'objectif du document est de fournir des lignes directrices pour l'établissement d'un PRIC des TI et des TO au sein d'une organisation.

Hypothèses

Ce document tient compte de quelques hypothèses sur l'état de votre organisation qui doivent être prises en considération :

- il existe déjà un PRIC pour les biens de TI, mais il n'est pas établi de manière à inclure les protocoles d'intervention de TO/système de contrôle industriel (SCI); et
- il existe déjà un plan de gestion de crise et de situations d'urgence de l'organisation.

Comprendre un environnement de TO

En établissant un PRIC qui couvre à la fois les biens axés sur la TI et sur la TO, il est important de comprendre quels biens liés à la TO vous pouvez avoir au sein de votre organisation. Cela signifie souvent qu'il faut d'abord définir ce que signifie la TO pour votre organisation, par exemple si elle inclut le contrôle des processus industriels, les caméras, l'infrastructure de la technologie informatique, les dispositifs de TO non connectés ou tout ce qui est simplement au-delà de la portée des TI.

Déterminer les biens de TO

Un bien de TO peut généralement être défini comme tout appareil physique ou logiciel utilisé pour contrôler, surveiller, configurer, recueillir des renseignements ou soutenir des systèmes de contrôle industriel (ou autres systèmes connexes). Dans les organisations principalement industrielles, il existe à la fois des points communs et des différences distinctes dans chacun des systèmes qui doivent être pris en compte afin de comprendre les biens organisationnels qui doivent être couverts par un PRIC des TI et des TO.

La mise en service d'un système qui comprend des composants de contrôle industriel inclut généralement des spécialisations en ingénierie, en électricité et en maintenance, en plus des composants informatiques qui peuvent être possiblement perturbés ou manipulés lors d'un cyberincident. Il est important de prendre en compte que les mêmes spécialistes utilisés lors de la mise en service peuvent également être nécessaires si le processus de contrôle industriel est compromis ou touché par un cyberincident.

Les organisations qui utilisent les technologies opérationnelles peuvent être de petite ou grande taille. L'inventaire des biens et les évaluations de risques de l'organisation sont des outils essentiels pour mieux identifier les systèmes qui relèvent de la compétence d'un PRIC.

Un SCI typique peut être composé des technologies suivantes :

Systèmes de protection	Protection des générateurs Protection des transformateurs Protection de la distribution d'électricité

Soutenir l'infrastructure technologique informatique	Équipement de réseautage associé (commutateurs, routeurs, pare-feu) Systèmes d'authentification et d'accès à distance Serveurs de journalisation, de surveillance et de gestion du système

Systèmes de contrôle	Systèmes de contrôle distribués (DCS) et composantes Systèmes de contrôleurs logiques programmables (PLC) Systèmes de contrôle des turbines (TCS) et composantes Systèmes instrumentés de sécurité (SIS)

SCADA, IHM, agrégation de données et systèmes d'ingénierie	Systèmes de salles de contrôle Systèmes et composants de l'interface humain-machine (IHM) Systèmes et composants SCADA Postes de travail d'ingénierie et ordinateurs portables

Systèmes environnementaux	Systèmes de surveillance continue des émissions

« …la cybersécurité ne constitue généralement pas l'élément central lors de la conception des systèmes de TO. »

Il est important de se rappeler que de nombreux composants du SCI énumérés ci-dessus peuvent manquer de mécanismes de protection de base, tels que l'authentification forte, l'autorisation, l'audit et la validation des entrées, car la cybersécurité ne constitue généralement pas l'élément central lors de la conception des systèmes de TO. Au lieu de cela, les protocoles et systèmes industriels sont souvent élaborés pour des réseaux de confiance ou isolés. La fiabilité et la disponibilité sont donc les principales priorités, sans égard à l'origine des instructions provenant du réseau numérique et sans pouvoir gérer les données d'entrée malformées. Pour cette raison, il est tout à fait possible qu'une cyberattaque simpliste sur un SCI provoque des dommages matériels importants.

« Quelles seront les répercussions sur mon organisation si ce service ou système n'est plus accessible? »

Cyberincidents

Afin de comprendre comment une organisation peut mieux protéger et servir ses systèmes, il est important de déterminer, avant qu'un incident ne se produise, quelles répercussions les cyberincidents ou cyberévénements peuvent avoir sur ces systèmes. La question fondamentale qui doit être posée pour gérer efficacement ces incidents à l'avance est la suivante : « Quelles seront les répercussions sur mon organisation si ce service ou système n'est plus accessible? »

Voici quelques exemples de scénarios qui illustrent comment les dépendances entre les systèmes de TI et de TO peuvent être exploitées par des cyberincidents, entraînant ainsi des répercussions négatives possibles sur les organisations industrielles. Tenez compte de ces scénarios lorsque vous répondez à la question ci-dessus :

- Un rançongiciel affecte un appareil fonctionnant sous Windows, ce qui a des répercussions sur les opérations dans un port de chargement. Les techniciens du port ne sont pas en mesure de surveiller et de contrôler les équipements essentiels aux opérations portuaires, de sorte que les opérations sont suspendues jusqu'à ce que l'appareil puisse être rétabli.
- Un attaquant exploite les outils d'accès à distance d'une organisation, tels que le réseau privé virtuel (RPV), et obtient un accès à distance non autorisé à un système essentiel. L'attaquant peut ainsi abuser des commandes de moteur et détruit les installations physiques de transformation des aliments, ce qui entraîne une perte d'inventaire et d'équipements.
- Un employé mécontent travaillant dans une centrale électrique abuse du système de gestion des changements pour modifier secrètement les paramètres de logique de verrouillage entre les contrôleurs de logique programmables, causant des dommages importants aux équipements et perturbant les opérations de la centrale.

Tous les scénarios ci-dessus sont susceptibles de faire appel à la fois aux équipes de TI et de TO en matière de scénarios d'intervention en cas d'incident, ce qui exigerait que les deux systèmes puissent s'organiser et travailler ensemble. Ces scénarios pourraient avoir des répercussions négatives graves sur l'une des organisations énumérées ci-dessus. Dans des situations et des événements comme ceux-ci, il est important que les organisations comprennent les ramifications possibles des perturbations cybernétiques dans leur secteur de responsabilité, et soient capables de s'organiser efficacement entre les disciplines technologiques (TI et TO) afin d'apporter les interventions nécessaires.

Évaluations des risques

Une évaluation des risques est un outil précieux qui favorise une compréhension plus complète des biens de TI et de TO qui composent une organisation. Diverses options d'évaluation sont possibles, y compris des options de source ouverte librement accessibles comme le Cyber Security Evaluation Tool (CSET) émis par le Department of Homeland Security (DHS) des États-Unis, jusqu'aux services payants des organisations professionnelles.

Lorsqu'une évaluation complète des risques est réalisée, il est important de réfléchir à la manière dont les risques peuvent être utilisés ou exploités pour nuire à votre organisation. Ce faisant, il est important de prendre en compte à l'avance ce qui suit :

- Quelles seront les conséquences des risques organisationnels sur les éléments suivants :
  - les équipements;
  - les procédés contrôlés;
  - les processus opérationnels;
  - les clients.
- Quelles sont les trajectoires d'attaque probables vers et à travers le réseau?
- Quelles sont les configurations de réseau de l'organisation et comment est-il possible de les contourner?
- Des pratiques de sécurité adéquates sont-elles en place et sont-elles correctement appliquées?

Autres points dont il convient de tenir compte :

- Examiner d'autres exemples de cyberincidents des TO réels et les conséquences qu'ils ont sur les organisations (coût, réputation, temps d'arrêt, etc.).
- Consulter les rapports de sécurité pertinents d'autres fournisseurs, industries et partenaires de confiance.
- Comparer les leçons retenues avec vos propres systèmes afin de trouver des solutions plus efficaces.

Comprendre la structure organisationnelle

Une fois que le rôle de l'équipe des TO est établi et que les répercussions possibles sur les SCI de l'organisation sont bien comprises, vous devez alors mieux comprendre la structure organisationnelle et comment une EIIC mixte des TI et des TO peut fonctionner au mieux dans ce contexte.

Il convient de noter qu'il n'existe pas de modèle unique qui puisse répondre adéquatement aux complexités et considérations particulières d'une organisation donnée, et que toute approche visant à établir une EIIC spécialisée ou intégrée doit refléter les besoins et la structure propres à l'organisation.

Structure organisationnelle

Une EIIC typique se compose de deux types de ressources principales : des ressources qui sont entièrement consacrées à l'intervention face aux événements et des ressources ayant d'autres fonctions principales qui sont ensuite élargies pour inclure l'intervention face aux événements selon les besoins (en fonction de la nature et de la portée de l'événement). Les organisations devraient également définir et attribuer les rôles avant qu'un incident ne se produise, afin d'éviter d'avoir à élaborer des procédures d'intervention pendant la gestion d'une crise.

Lors de l'évaluation de la structure organisationnelle, déterminez tous les autres services et domaines qui pourraient être liés à un cyberévénement ou à un cyberincident ou être touchés par l'un ou l'autre, afin de mieux comprendre tous les efforts d'intervention qui pourraient être nécessaires.

« La connaissance des compétences en TI et en TO actuellement présentes au sein de l'organisation aidera à comprendre les ressources qui doivent être organisées, ce qui contribuera à la mise en place d'une EIIC efficace. »

Identifiez toute caractéristique unique des systèmes desservis par l'EIIC, comme la composition de l'équipe, l'emplacement et la distribution physique et géographique, et le secteur dans lequel l'organisation opère. La structure du plan d'intervention à choisir dépendra également des facteurs suivants :

- la taille de l'organisation;
- le nombre de lieux géographiques;
- les systèmes et plateformes qui appuient l'organisation;
- les services qui doivent être offerts par l'équipe d'intervention en cas d'incident;
- l'expertise technique des membres du personnel en place.

La connaissance des compétences en TI et en TO actuellement présentes au sein de l'organisation aidera à comprendre les ressources qui doivent être organisées, ce qui contribuera à la mise en place d'une EIIC efficace.

Membres de l'EIIC

Après avoir bien compris les systèmes qui existent au sein d'une organisation dans la section précédente, vous devez ensuite cibler les membres de l'EIIC de votre organisation. Il faut tenir compte de l'expertise technique requise pour exécuter les tâches particulières liées aux diverses activités d'intervention en cas d'incidents, de manière à choisir les membres de l'EIIC en fonction de leurs capacités, de leurs compétences et de leur expertise au sein de l'organisation. Les autres membres de l'équipe peuvent inclure des représentants des services juridiques, des ressources humaines, des relations publiques, de la gestion des risques, des fournisseurs et des ressources d'application de la loi et des enquêtes criminelles.

Il est également viable d'envisager des ententes de sous-traitance, comme des ententes avec des fournisseurs de service de gestion et de maintenance, des centres d'opérations de sécurité et des sociétés d'intervention en cas d'incident. Comme la technologie repose de plus en plus sur de multiples disciplines, il est donc important de s'assurer à l'avance que leurs fonctions et capacités connexes sont correctement intégrées dans le plan d'intervention. Enfin, un élément ou une structure de gestion doit être mis en place pour orienter l'équipe en cas de crise. Ces éléments sont expliqués davantage ci dessous.

Le gestionnaire de l'EIIC : Le gestionnaire de l'EIIC sera la première personne à intervenir en cas d'incident et maintiendra un lien hiérarchique continu avec les représentants de la haute direction. Cela

peut exiger de rendre compte au dirigeant principal de l'information (DPI), au dirigeant principal de la sécurité (DPS), à l'agent principal de gestion du risque (APGR) ou à tout autre responsable équivalent. Le responsable de l'équipe d'intervention en cas d'incident est essentiel pour s'assurer que tous les incidents sont traités de manière responsable et imputable, afin de gérer plus directement les incidents. Bien que le gestionnaire de l'EIIC soit particulièrement essentiel lors d'un incident, il est important de s'assurer que l'organisation dans son ensemble profite de formation continue, d'un programme de perfectionnement et de sensibilisation générale en matière de cybersécurité et d'intervention en cas d'incident lorsque ceux-ci ne se produisent pas.

Intervenants de l'équipe d'intervention en cas d'incident : Les intervenants de l'EIIC peuvent être des personnes embauchées précisément pour remplir le rôle d'un membre consacré à l'équipe d'intervention en cas d'incident, et partageront les rôles au sein de l'organisation, des ressources externes, ou une combinaison de celles-ci. Ils peuvent également posséder diverses compétences qui répondent aux divers besoins de l'organisation, et devraient être assignés à des rôles en fonction de la gravité de l'événement, s'il se produit. Il est important de noter que tous les membres de l'EIIC ne sont pas nécessaires pour chaque incident, et la même personne peut remplir plusieurs rôles au sein de l'EIIC, en fonction des considérations particulières de l'organisation ou de l'ampleur de l'incident.

Adopter une approche centralisée ou décentralisée

La décision d'adopter une approche centralisée ou décentralisée d'intervention en cas d'incident dépendra largement de la structure de l'organisation en question. Les deux modèles sont examinés ci dessous.

Approche centralisée

Un modèle centralisé exige une proximité avec l'entité, soit physiquement, soit géographiquement. Dans un modèle centralisé, les ressources sont normalement situées dans le même bâtiment ou le même complexe que les biens des TI et des TO, et sont responsables de toutes les activités de gestion des incidents au sein de l'organisation. Avec ce modèle, il y a une EIIC spécialisée, dotée d'un personnel complet, qui traite tous les incidents au sein d'une organisation. Cela signifierait que les membres de l'équipe passeraient 100 % de leur temps à travailler pour l'EIIC. Le choix d'un modèle centralisé dépend donc de la taille et de la complexité de l'organisation, et du fait que celle-ci ait ou non constamment besoin d'intervenants dédiés à la gestion des incidents. Une organisation plus importante profitera d'une approche centralisée, étant donné l'hypothèse générale selon laquelle une taille plus importante entraînera souvent une exposition accrue au risque.

Approche décentralisée

Un modèle décentralisé existe lorsque l'entité n'est pas située dans les mêmes bâtiments, villes, pays, régions géographiques ou fuseaux horaires. Il exige une approche différente de celle du modèle centralisé, dans la mesure où le modèle décentralisé est plus souple et agile. Une organisation utilisant un modèle décentralisé utilise les membres du personnel existants pour fournir une « EIIC virtuellement répartie ». Les membres de l'équipe sont souvent des personnes dont le rôle principal est en dehors de l'intervention en cas d'incident, et leur rôle est attribué à un ensemble de compétences, un niveau d'expertise ou un lieu géographique particulier. Ils sont appelés à apporter leur appui à l'équipe d'intervention en cas d'incident lorsqu'un incident se produit.

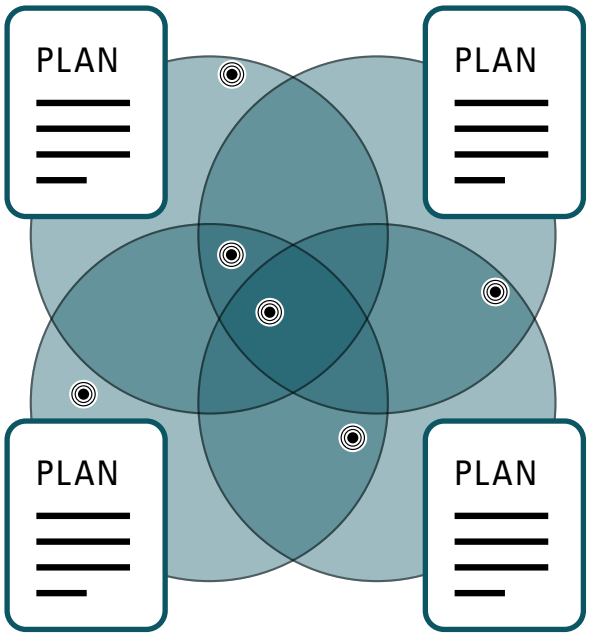
Options de structure organisationnelle pour la conception du plan d'intervention en cas de cyberincident

Il est possible de structurer un plan mixte d'intervention en cas de cyberincident des TI et des TO de différentes manières. Les plans peuvent tous être liés et peuvent s'appuyer les uns les autres en fonction de la façon dont un incident technologique survient dans l'organisation. En outre, les plans mixtes d'intervention en cas de cyberincident des TI et des TO peuvent être harmonisés de manière à ce qu'ils s'appuient mutuellement.

Comme mentionné précédemment, un plan d'intervention en cas de cyberincident complémente et fonctionne avec d'autres plans d'intervention à l'échelle de l'organisation comme les plans de gestion de crise ou de situations d'urgence. Dans une organisation décentralisée, il est possible que les cyberincidents aient diverses répercussions qui touchent de petites zones d'un même site ou l'ensemble de l'organisation lors d'un seul incident. Il est également possible qu'un incident technologique entraîne une crise ou une situation d'urgence à l'échelle de l'organisation, ou qu'une crise ou une situation d'urgence nécessite une intervention en cas de cyberincident. Tous ces scénarios exigent des plans d'intervention multiples qui peuvent être liés.

Un événement peut affecter à la fois le domaine des TI et des TO. Ainsi, les plans doivent fonctionner de manière isolée mais aussi ensemble si nécessaire.

Les incidents peuvent déclencher un seul plan ou plusieurs plans simultanément



La découverte par la pratique!

Un exercice (fonctionnel ou de simulation) peut être un moyen efficace de déterminer l'approche qui sera nécessaire pour gérer correctement un incident dans votre organisation. Cela peut également vous permettre de mieux comprendre la structure réelle de votre organisation, ainsi que les capacités dont vous disposez pour répondre à un incident. À l'aide des exercices, il est possible de déterminer à la fois les forces et les faiblesses de votre organisation. Une analyse ultérieure permet de déterminer la structure qui répond le mieux aux besoins particuliers de votre organisation.

Pour savoir si une approche décentralisée ou une approche centralisée fonctionnera mieux pour votre organisation, tenez compte des points suivants :

« Toutes les organisations sont différentes, et l'approche dépendra des besoins propres à votre organisation. »

- toutes les organisations sont différentes, et l'approche dépendra des besoins propres à votre organisation;
- les organisations fortement dispersées peuvent envisager d'avoir des plans individuels adaptés à chaque unité opérationnelle qui renvoient tous à un plan directeur à l'échelle de l'organisation;
- les organisations plus intégrées peuvent envisager de mettre en place une équipe de spécialistes en matière d'intervention en cas d'incident, avec un plan de coordination central;
- les exercices de simulation sont d'excellents moyens de mettre vos plans à l'essai.

Prenez un point de vue de TO

Différences entre les systèmes de réseaux de TI et de TO

Bien que les TI et TO se chevauchent et soient complémentaires, il est recommandé de prendre le temps de discuter de certaines des principales différences entre les deux systèmes avant de mettre en œuvre une EIIC unie.

Les réseaux de TI et de TO diffèrent en matière d'infrastructure, de technologie, de fournisseurs, de protocoles et d'environnement physique, et exigent donc différents types de compétences, de formations et d'exigences de sécurité. Une approche propre à la TI exercée dans le cadre d'un incident de TO n'est pas nécessairement la meilleure solution, si la technologie est fondamentalement différente pour chaque système.

Les environnements physiques des réseaux de TI et de TO sont également différents. Un réseau de TI est souvent accessible depuis un bureau, alors qu'un réseau de TO tend à se trouver dans un environnement industriel. Cela signifie que les réseaux de TO sont généralement décentralisés et peuvent être situés dans des zones très éloignées, souvent à côté des équipements que le réseau et les dispositifs connexes contrôlent.

Technologie de l'information	vs.	Technologie opérationnelle
La priorité est la confidentialité		La priorité est la disponibilité et l'intégrité
Le temps n'est pas un facteur critique		En temps réel
Technologies récentes / Mises à jour fréquentes		Technologie éprouvée / Mise à jour peu fréquente
Produits de consommation		Petit marché spécialisé
Mettre à jour maintenant		Mettre à jour plus tard peut-être
Modifications librement autorisées - test sur le terrain		Modification difficile - prouver la non-intervention, requalifier, tester en ligne
Redémarrage à tout moment		Redémarrages planifiés et coordonnés
Surveillance et diagnostic en ligne du système		Surveillance et diagnostic limités du système
Accès physique à tout moment		Accès limité - peut-être seulement pendant les pannes
Faiblesse des processus de suivi des actifs et de contrôle des changements		Des exigences réglementaires strictes et un contrôle rigoureux des changements
Nécessite généralement un accès à Internet pour l'octroi de licences et les mises à jour		Augmenter l'accès à l'internet autorisé
Permet la maintenance et l'assistance à distance		Augmenter les niveaux d'accès à distance
L'impact de l'échec est en heures-personnes		L'impact de la défaillance est la sécurité et la production
Une forte culture de la sécurité		Une forte culture de la sûreté (sécurité)

Formation en sécurité

Selon le contexte et les exigences propres à votre organisation, une EIIC peut être tenue de certifier les employés dans le cadre d'une formation supplémentaire en matière de sécurité qui traite des risques particuliers associés au travail dans un environnement centré sur la TO. La formation en matière de sécurité doit être maintenue dans la mesure du possible, afin de contribuer à réduire les délais d'intervention des intervenants qui doivent travailler dans des environnements de TO.

Idéalement, la première fois qu'un intervenant est tenu de porter un casque de protection lorsqu'il entre dans une installation ne devrait pas être lors d'une intervention dans le cas d'un incident réel. Ce type d'exigences, en l'occurrence la nécessité de porter un équipement de protection individuelle, doit être pris en compte dans la mise sur pied initiale de l'équipe et enseigné en même temps que la formation des capacités techniques nécessaires.

Répercussions sur la résilience

La triade C-I-D (confidentialité, intégrité et disponibilité) propre à la sécurité de l'information est souvent utilisée comme jauge pour évaluer la sécurité d'un environnement de TI. Cependant, dans les environnements de TO, l'accent est moins mis sur la « confidentialité », car il faut une latence plus faible et un temps utilisable de 100 % (c'est-à-dire la « disponibilité »). La triade C-I-D diffère également pour les environnements de TO dans la mesure où il existe une interdépendance entre les organisations, ce qui pourrait avoir un effet en cascade sur d'autres systèmes, d'autres intervenants et même d'autres nations. Prenons l'exemple du réseau électrique nord-américain, et la façon dont il est intégré et connecté entre des États, provinces et pays différents. Étant donné ce type d'interdépendance, un incident pourrait avoir des répercussions en cascade sur de nombreux autres.

En raison de ces différences essentielles, les équipes d'intervention en cas d'incident au sein d'un réseau de TO doivent prendre en considération plusieurs facteurs géographiques, techniques et parfois politiques qui sont propres à un environnement de TO. En raison de cette exigence, et particulièrement pour des infrastructures critiques où la sécurité et le bien-être des citoyens sont souvent en jeu, les différences suivantes liées aux environnements de TO devraient être suffisamment prises en compte :

- **La nature propriétaire de la technologie :** Le matériel et les logiciels de TO sont souvent de nature propriétaire, ce qui exige que les intervenants en cas d'incident soient familiarisés et aient de l'expérience avec différents types d'environnements

« Il faut connaître son environnement, et élaborer des trousses d'intervention en conséquence.

d'exploitation. De nombreux produits matériels sont « renforcés » ou autrement adaptés à différents environnements ou conditions de fonctionnement, et les méthodes traditionnelles de collecte des données d'intervention en cas d'incident peuvent devoir être adaptées en conséquence. Il faut tenir compte du fait que les boîtes à outils utilisées pour l'intervention en cas d'incident dans un environnement de TI ne fonctionnent pas nécessairement pour un environnement de TO pour la même raison. Il faut connaître son environnement, et élaborer des trousses d'intervention en conséquence.

- **Le cycle de vie des produits :** Contrairement aux systèmes de TI traditionnels, les équipements informatiques de TO ont généralement un cycle de vie plus long, soit environ 10 à 15 ans. Par conséquent, les techniques d'intervention en cas d'incident dans les systèmes de TI, qui sont normalement mieux adaptées aux systèmes d'exploitation modernes, devront être adaptées lorsqu'elles seront appliquées à un environnement axé sur la TO. Par exemple, les intervenants en cas d'incident devront être outillés de compétences en matière d'enquête sur les données allant de Windows XP à Windows 10, et tout ce qui se trouve entre les deux (ou même des versions plus vieilles!).
- **Outils et techniques d'intervention en cas d'incident :** Quel que soit l'environnement (TI ou TO), tous les outils ou processus utilisés en matière d'intervention en cas d'incident doivent être mis à l'essai et validés pour être utilisés dans le réseau désigné. Les environnements de TO sont souvent très sensibles et incapables de maintenir des activités de balayage soutenues, voire même la simple exécution de Network Mapper (NMap) qui peut entraîner de graves conséquences. La collecte, le stockage et la récupération des journaux sont également différents dans les environnements de TI et de TO. Comme il s'agit d'une source principale pour déterminer la cause première au cours d'une enquête, il est important que les intervenants connaissent et maîtrisent les techniques de collecte et d'enquête correspondantes.

La volonté de mettre en lumière les principales différences entre les systèmes de TI et les systèmes de TO n'est pas de créer une division entre les deux groupes, mais plutôt de favoriser un sentiment de compréhension entre les deux domaines lors de l'élaboration d'un plan mixte d'intervention en cas d'incident des TI et des TO. La promotion d'une culture de compréhension et de collaboration entre les groupes de TI et de TO peut être renforcée par des événements tels que des ateliers ou des dîners transculturels, où chaque groupe peut présenter et échanger des renseignements sur sa réalité et acquérir une appréciation et une compréhension des fonctions professionnelles des uns et des autres.

Élaboration d'un plan mixte d'intervention en cas de cyberincident des TI et des TO

Une fois qu'une meilleure compréhension de la structure, des besoins et des circonstances d'une organisation est acquise et qu'il a été décidé d'aller de l'avant avec la mise en place d'un plan mixte d'intervention en cas d'incident des TI et des TO, il est recommandé de mettre en place la capacité opérationnelle à l'aide des étapes suivantes :

Étape 1 : Constituer une équipe interfonctionnelle

L'élaboration d'un plan mixte d'intervention en cas de cyberincident des TI et des TO réussi exige la participation des principaux intervenants qui travaillent à la fois dans les environnements de la TI et de la TO de l'organisation. À ce stade initial de la planification, il est essentiel de bien déterminer et définir les rôles de ceux qui ont ou auront le pouvoir et la capacité de décision lors d'une intervention en cas de cyberincident. Les points suivants doivent être considérés :

- **Examiner** les plans d'intervention de l'organisation en cas de crise et d'urgence. Si ceux-ci existent, les rôles et les responsabilités y sont peut-être déjà définis, ce qui fera en sorte qu'il ne sera pas nécessaire de les concevoir à partir de zéro. Si ce n'est pas le cas, il faudra clarifier davantage les rôles et les responsabilités (voir l'étape 2 ci-dessous pour plus de renseignements).
- **Mener** des entretiens ou des ateliers avec des responsables dans les domaines de l'ingénierie, des opérations, de la haute direction, etc., en utilisant différents scénarios de confinement pour tester l'efficacité de l'intervention. Le fait d'axer les entretiens et les ateliers sur l'évaluation des répercussions sur la sûreté et les opérations peut apporter une aide supplémentaire dans les cas où une bonne compréhension des questions de cybersécurité fait défaut dans le contexte de la TO de l'organisation. Mettre l'accent sur les différentes compétences et sur l'expertise dans chaque domaine de l'organisation peut aider à faire valoir différentes perspectives et contributions. Cela peut contribuer à appuyer l'intervention en cas

d'incident et à faciliter le dialogue nécessaire qui pourrait en fin de compte aider à la prise de décisions.

- **Examiner** les leçons retenues des cyberincidents passés qui se sont produits au sein de l'organisation, et tirer parti des renseignements obtenus grâce aux expériences passées. Cela peut fournir un contexte et de précieux renseignements sur la manière dont les incidents précédents ont été traités, ce qui peut aider à définir les différents rôles et les équipes nécessaires pour intervenir en cas d'incident de TO à l'avenir.

Étape 2 : Examiner tout plan d'intervention en cas d'incident existant au sein de l'équipe

L'objectif principal de cette étape est de tirer parti des plans d'intervention en cas d'incident qui peuvent déjà exister dans l'organisation et qui peuvent souvent servir de point de départ pour l'élaboration d'un plan mixte d'intervention en cas de cyberincident des TI et des TO. Il est important de reconnaître qu'aucun plan d'intervention en cas d'incident n'existe en vase clos, et qu'une approche véritablement coordonnée en matière de risque ne peut être obtenue qu'en unifiant les différentes capacités et équipes à tous les niveaux de l'organisation. Les étapes suivantes doivent être prises en compte lors de l'examen des plans d'intervention en cas d'incident existants dans l'organisation :

« ...une approche véritablement coordonnée en matière de risque ne peut être obtenue qu'en unifiant les différentes capacités et équipes à tous les niveaux de l'organisation. »

1. Déterminer les plans d'intervention en cas d'incident préexistant (physiques ou cybernétiques). Il peut s'agir de plans d'intervention liés à différents domaines, notamment :
   - la TI;
   - la TO;
   - la sécurité physique;
   - l'intervention en cas de crise ou de situations d'urgence (santé et sécurité, environnement, etc.);
   - la continuité des opérations.
2. Organiser une discussion ouverte ou mener un exercice de simulation avec la participation du personnel de sécurité concerné, par exemple :
   - les dirigeants principaux de l'information;
   - les programmeurs en automatisation et ingénieurs de procédés;
   - la sécurité de l'information et de la TI;
   - la sécurité physique;
   - les conseillers juridiques;

- les communications organisationnelles
- les autres entités concernées, le cas échéant.

3. Examiner tout plan existant dans le cadre d'un plan mixte d'intervention des TI et des TO, en gardant à l'esprit les points suivants :
   - la définition organisationnelle d'un « incident » doit être largement comprise, tout en reconnaissant que ce qui constitue un incident dans un domaine peut ne pas être applicable à un incident qui a lieu dans un autre;
   - il est possible que les incidents technologiques diffèrent par leur niveau d'incidence, car ils peuvent aussi bien toucher une petite partie d'un emplacement unique qu'une organisation entière;
   - les incidents peuvent être à la fois matériels et cybernétiques, chacun ayant la capacité d'avoir des conséquences sur l'autre;
   - s'il existe actuellement une plateforme ou un procédé permettant de suivre activement et historiquement les incidents, il convient d'y faire référence pour trouver des points communs;
   - il faut déterminer s'il existe des domaines où il est judicieux de maintenir les plans de TI et de TO séparés les uns des autres, et inversement, où il est logique de les combiner;
   - si les équipes d'intervention de la TI et de la TO sont distinctes, déterminez s'il existe des domaines dans lesquels l'une des équipes peut aider l'autre lors d'une intervention;
   - il faut déterminer s'il existe des outils, des systèmes ou des termes utilisés à la fois par les équipes de la TI et de la TO, et déterminer quand et comment ces ressources partagées peuvent être utilisées pour cibler d'éventuels domaines d'amélioration.

4. S'il n'existe pas de plan d'intervention en cas d'incident ou de ressources au sein d'une organisation, envisager les options suivantes comme sources de référence possibles :
   - des plans d'intervention en cas d'incident en ligne;
   - des solutions fournies par des fournisseurs;
   - des modèles fournis par les fournisseurs de cyberassurance;

Il est également important de noter que certaines organisations peuvent avoir des approches « maison » ou « de base » pour réagir aux incidents. Ces processus ne sont pas nécessairement considérés comme une politique organisationnelle officielle, mais ils peuvent refléter les méthodes et les procédures qui fonctionnent bien pour l'organisation. Si de telles politiques, procédures opérationnelles standards (POS) ou ententes existent, il est essentiel de les revoir, afin qu'elles puissent être prises en compte tout au long de l'élaboration d'un plan d'intervention commun en cas d'incident touchant les TI et TO.

Étape 3 : Définition d'un incident

Il sera important de comprendre et de définir à quoi peut ressembler un incident pouvant déclencher le plan d'intervention en cas d'incident au sein de votre organisation. Par exemple, un petit incident qui touche un seul système sera certainement un sujet d'enquête, même s'il n'est pas nécessaire de recourir au plan d'intervention en cas d'incident.

En outre, votre organisation peut juger nécessaire de définir la différence entre un événement et un incident pour vous aider à savoir quand recourir au plan d'intervention en cas d'incident.

- **Cyberévénement :** toute action, interaction et tout comportement observables dans un environnement de systèmes (p. ex., trafic de réseau, processus de système ou comportement des applications).
- **Cyberincident :** tout événement intentionnel ou non intentionnel de cybersécurité qui compromet ou tente de compromettre la confidentialité, l'intégrité ou la disponibilité d'un système, d'un réseau ou d'une information numérique.

Remarque : votre cadre réglementaire peut comporter des définitions plus précises qui se rapportent à votre environnement particulier, et les utilisateurs de ce guide sont incités à consulter ce matériel.

Les exemples suivants illustrent la différence entre les événements et les incidents :

- Exemples de **cyberévénements :**
  - Utilisateur connecté à un partage de fichiers;
  - Utilisateur se connectant à un système;
  - Échec de la connexion d'un utilisateur en raison d'un mauvais mot de passe;
  - Demande HTTP.
- Exemples de **cyberincidents :**
  - Comportement inhabituel à partir d'un compte privilégié;
  - Tentatives d'hameçonnage par courriel;
  - Trafic réseau non autorisé observé par un hôte externe;
  - Violations du processus de gestion du changement.

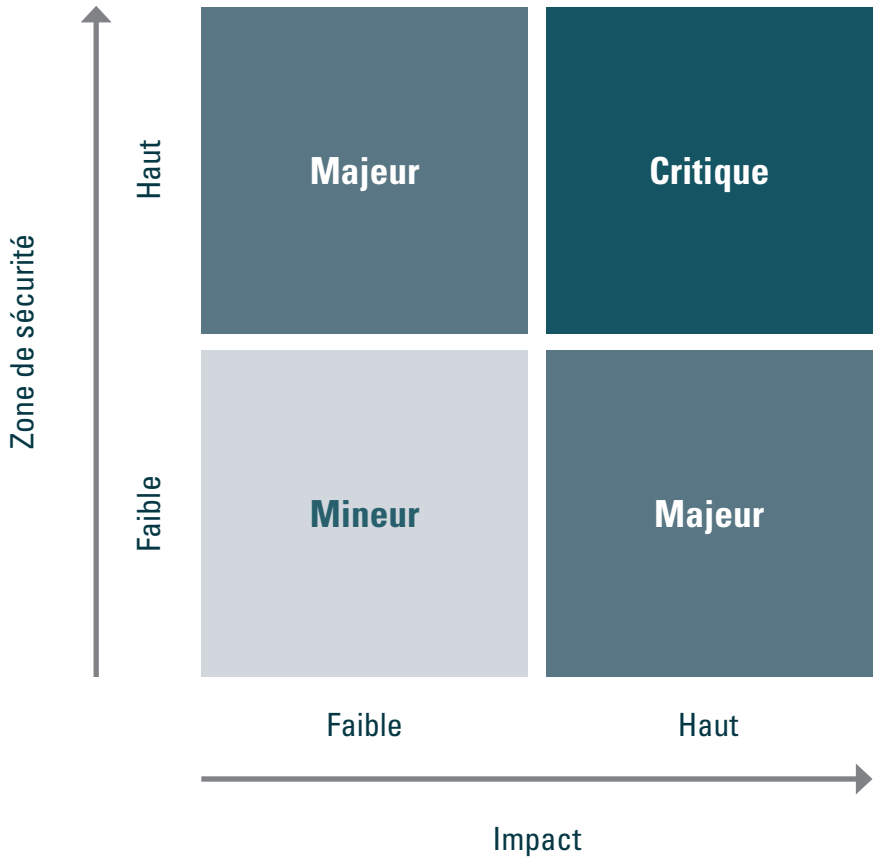
Classification de la gravité des incidents

La classification d'un incident aidera à déterminer s'il est nécessaire de recourir au plan d'intervention en cas d'incident. Afin de classer le niveau de gravité d'un incident, l'EIIC doit tenir compte de la zone de sécurité où l'incident a lieu, et de l'impact ou de l'impact potentiel sur l'organisation ou sur la zone où l'incident se produit.

La matrice de classification présentée ci-dessous montre une façon d'utiliser la relation entre les zones de sécurité et l'incidence pour déterminer le niveau de gravité d'un incident. Le plan d'intervention en cas d'incident

au sein d'une organisation doit comprendre différentes méthodes pour répondre à différents incidents, en fonction de leur niveau de gravité, comme l'illustre le schéma suivant :

Matrice de classification de la gravité des incidents dans les TI et les TO



- **Zone de sécurité :** regroupement physique et logique d'un ou de plusieurs actifs TI et TO ayant, dans une organisation, les mêmes exigences (ou des exigences similaires) en matière de cybersécurité
- **Incidence :** une estimation des pertes potentielles ou réalisées associées à un incident identifié pour une organisation ou pour la sécurité publique

Étape 4 : Déterminer comment les équipes vont s'assembler

Cette étape permet de définir les différentes équipes qui devraient être engagées dans une EIIC commune dans les TI et les TO. Au minimum, deux grands rôles d'équipe devraient être choisis pour gérer les incidents de sécurité informatique d'une organisation :

1. L'équipe d'intervention en cas des incidents cybernétiques (EIIC);
2. L'équipe de la haute direction et de gestion de crise.

L'équipe d'intervention en cas d'incidents de sécurité informatique

L'EIIC devrait être composée de membres des TI et des TO ayant une expertise en la matière et pouvant enquêter sur les incidents, déterminer et mettre en œuvre les mesures de confinement et d'assainissement appropriées pour résoudre la situation. Cette équipe peut comprendre (le cas échéant) des membres de :

- Diverses disciplines en TI, notamment :
  - L'équipe chargée de la cybersécurité des TI;
  - L'architecture d'entreprise;
  - L'infrastructure des systèmes de TI (soutien réseau, serveur et bureautique);
  - Service d'assistance en TI (ou centre d'assistance);
  - Propriétaires des systèmes concernés.
- Les équipes des systèmes de TO, notamment :
  - L'équipe de cybersécurité des TO;
  - Infrastructure des systèmes de TO (réseau, serveur);
  - Programmeurs industriels et spécialistes des systèmes de TO (selon les besoins);
  - Partenaires en ingénierie (internes ou tierces parties).
- Fournisseurs de services gérés (le cas échéant) :
  - Analystes du Centre des opérations de sécurité sous-traité;
  - Fournisseurs de services en nuage (le cas échéant);
  - Les partenaires d'intervention en cas d'incidents (p. ex., les spécialistes de l'analyse judiciaire).

L'EIIC devrait avoir un responsable désigné (ou commandant de l'incident) qui sera chargé de prendre des décisions importantes et de remédier à des problèmes tels que :

- Développer et maintenir des processus d'intervention en cas d'incidents de cybersécurité, en décrivant le processus d'intervention, comment et quand engager les intervenants internes et externes, et quand engager l'équipe de la haute direction et de gestion de crise;
- Définir et attribuer les rôles et responsabilités des membres de l'EIIC;
- Déclarer les incidents lorsqu'ils se produisent et invoquer le processus d'intervention lors d'incidents cybernétiques (si nécessaire);
- Maintenir les outils nécessaires pour avoir recours à l'EIIC (si nécessaire);
- Maintenir les coordonnées de tous les membres, ainsi que de l'équipe de la haute direction et de gestion de crise et autres parties externes (si nécessaire);
- Avoir recours à l'EIIC, enquêter sur les incidents et assurer la liaison avec les intervenants concernés (si nécessaire);
- Signaler et assurer la liaison avec l'équipe de la haute direction et de gestion de crise (le cas échéant);

L'équipe de la haute direction et de la gestion de crise

L'équipe de la haute direction et de gestion de crise sert de liaison principale nécessaire dans le cas d'un incident touchant les TI et les TO. L'équipe de la haute direction et de gestion de crise s'emploie à coordonner les communications avec les parties externes, les forces de l'ordre, les autres équipes d'intervention en cas d'incident, les hauts responsables, les ressources humaines, le conseil d'administration, le conseiller juridique, la conformité, etc. Cette équipe doit (le cas échéant) comprendre ce qui suit :

- La haute direction des TI et des TO;
- Un conseiller juridique;
    - Fournir un soutien juridique selon les besoins ou les demandes de l'EIIC.
    - Fournir des conseils à l'équipe en ce qui concerne les lois et les règlements régissant les opérations de l'équipe et les ramifications juridiques d'incidents particuliers.
    - Aider à garantir que les preuves relatives aux violations de la politique soient correctement recueillies et qu'une chaîne de possession soit maintenue.

- Fournir des orientations sur les violations de données qui peuvent faire l'objet de mandats de déclaration de conformité législative ou réglementaire.
- S'assurer que les exigences relatives à la cyberassurance sont respectées (si l'organisation a souscrit une police de cyberassurance).

- Département des finances;
  - Travailler avec tout fournisseur de cyberassurance pour s'assurer que les services de couverture de cyberassurance sont utilisés et que la procédure de réclamation est suivie.

- Communications organisationnelles;
  - Fournir un soutien en matière de communication, comme demandé par l'EIIC (et comme approuvé par l'équipe de la haute direction et de gestion de crise).

- Ressources humaines;
  - Fournir des conseils sur les incidents concernant l'utilisation inappropriée, les menaces internes, etc. du point de vue des ressources humaines.

Étape 5 : Déterminer comment les équipes communiqueront

Une communication efficace entre tous les intervenants clés de l'organisation est un élément essentiel lors de tout type d'incident ou d'événement. Les organisations doivent établir un plan de communication commun comprenant des seuils d'escalade qui garantiront un engagement approprié des principaux intervenants, allant du personnel de soutien technique aux équipes de la haute direction.

Les besoins de communication varieront pour chaque niveau d'une organisation en fonction de l'état d'urgence; il est impératif que des salles de réunion ou des ponts de conférence soient désignés pour les urgences. D'autres formes de canaux de communication devraient également être établies pour faciliter les efforts de coordination entre les niveaux appropriés de l'organisation.

L'organisation doit conserver la possibilité de déplacer le personnel de gestion des urgences vers d'autres lieux de travail (si possible), dans le cas où les lieux principaux seraient compromis ou inutilisables.

Une organisation doit comprendre que les cyberincidents peuvent avoir un impact sur les mêmes systèmes numériques qui sont utilisés pour la communication dans des circonstances normales. Par exemple, le réseau sous-

jacent lui-même peut être touché ou isolé pour réduire la propagation d'un virus numérique afin de protéger d'autres systèmes, ou des outils logiciels de collaboration peuvent être liés à des comptes d'administrateurs de systèmes compromis, les rendant inaccessibles.

Le plan devrait prévoir plusieurs *alternatives* de communication fiables et sûres pour les participants à l'EIIC, et ce, à chaque niveau. Il devrait contenir des instructions spécifiques pour chaque solution de rechange, au cas où les principales méthodes de communication ne seraient plus disponibles pendant l'incident (exemple : l'accès à l'internet ou le système de courriel ne sont pas disponibles).

Voici des exemples d'autres moyens de communication :

1. Un portail Web sécurisé sur l'Internet public avec des systèmes d'authentification distincts
2. Des connexions Internet secondaires et tertiaires, comme la téléphonie cellulaire ou le satellite
3. Un courrier électronique avec des listes de distribution prédéterminées pour les interventions lors d'incidents
4. Des systèmes de collaboration basés sur Internet ou ponts d'audioconférence
5. Des téléphones mobiles
6. Des lignes terrestres (ou « simple service téléphonique conventionnel »)
7. Des téléphones satellites
8. Des systèmes radio VHF/UHF

L'organisation doit définir des protocoles et des procédures spécifiques pour le personnel local du site. Elle doit aussi désigner un commandant d'incident local (c'est-à-dire une personne sur le terrain), au cas où la communication avec le commandement central de l'incident serait perturbée.

Certains seuils doivent également être définis. En outre, le pouvoir de décision délégué pour diverses situations doit être clairement identifié pour garantir une intervention autonome lors d'incidents de cybersécurité à distance. L'EIIC devrait établir des modèles de communication prédéterminés et offrir des conseils appropriés sur le type et le niveau d'information à fournir à chacun des forums suivants : équipes techniques, cadres intermédiaires, hauts dirigeants, partenaires de l'industrie, équipe d'intervention en cas d'urgence informatique, public, etc. Des protocoles d'examen et d'approbation appropriés devraient également être établis pour permettre la diffusion des informations aux autres participants,

partenaires et intervenants, dans la mesure où elles concernent l'incident et l'impact potentiel qui en résulte.

Étape 6 : Déterminer les mesures d'intervention nécessaires

L'objectif principal de cette étape est de déterminer la nature de tout incident ou événement cybernétique qui se produit dans un environnement de systèmes de contrôle industriels (SCI), et de définir les réponses appropriées visant à donner la priorité à la sécurité des personnes et à la fiabilité des opérations industrielles lors d'un incident. Les informations suivantes doivent être prises en compte lors de la mise en place ou de la conduite d'interventions lors d'incidents cybernétiques dans un cadre industriel.

Remarque : ce guide suppose que les réseaux SCI, y compris le Système de sécurité instrumenté, sont déjà correctement segmentés des réseaux d'entreprise, que les outils d'intervention lors d'incidents ont été testés pour garantir la sécurité d'utilisation du SCI et qu'une cyberposition défendable a été établie et testée.

Triage des menaces

Le personnel d'intervention lors d'incidents affectant les SCI doit rapidement trier et déterminer la portée d'un incident dès qu'il se produit. Il s'agit d'abord de comprendre les types de menaces auxquels on est confronté, le comportement des menaces, les vecteurs et les objectifs potentiels de la menace. Cela permettra de déterminer les mesures d'intervention appropriées nécessaires. Les données informatiques seront rapidement collectées (sur une période de deux à cinq heures) et analysées (sur une période de deux à cinq heures) pour déterminer la nature de la menace et la manière d'aborder les étapes de confinement et d'éradication. L'analyse des données consisterait en une analyse dynamique des logiciels malveillants et en une analyse statique des fichiers de propriété, une ingénierie inverse plus détaillée ayant lieu à un stade ultérieur. Il faut également commencer par recueillir des éléments de preuve sur les actifs essentiels du SCI, en priorisant généralement :

- Les contrôleurs de logique programmable (PLC) (vérification de la modification récente de la logique Ladder et identification des deltas à partir des hachages numériques des fichiers de projet obtenus précédemment);
- Les changements de compte ou de processus des historiens des données (les historiens des données sont un point chaud utilisé par les adversaires pour pivoter);
- Les interfaces humain-machine (IHM) de Microsoft Windows;

« Les incidents liés aux SCI sont rarement de courte durée, et il faut parfois des jours ou des semaines pour se défendre contre de futures attaques. »

- Les journaux d'accès à distance (tels que protocole de bureau à distance [RDP], RPV, etc.).

De plus, déterminez si des ressources supplémentaires (internes ou externes) sont nécessaires pour assurer la défense pendant l'attaque. Les incidents liés aux SCI sont rarement de courte durée, et il faut parfois des jours ou des semaines pour se défendre contre de futures attaques. Le nombre de personnes, les quarts de travail et la logistique doivent être envisagés en fonction de votre équipe de sécurité actuelle, ainsi que tout service d'intervention externalisé lors d'incidents, en vue d'augmenter vos capacités de réaction.

Établissement d'une cyberposition défendable pour l'intervention lors d'incidents liés aux SCI

Les outils utilisés pour les incidents reliés aux SCI comprennent des logiciels et du matériel d'acquisition de données pour l'analyse judiciaire des systèmes d'exploitation, l'ingénierie des données des appareils de terrain et la capture du trafic réseau; ils sont essentiels à toute stratégie défensive efficace. Il est important de tester tout outil avant qu'un incident réel ne se produise, non seulement pour évaluer la capacité de l'outil, mais aussi pour évaluer l'impact. L'objectif d'une cyberposition défendable est d'isoler autant que possible les opérations, lorsqu'on peut le faire, afin de s'assurer que les menaces potentielles aux opérations aient un impact réduit. Cela pourrait signifier la déconnecter le réseau TO du réseau TI d'entreprise, une zone démilitarisée de TO ou d'applications commerciales, ou la segmentation au sein du réseau de SCI (c'est-à-dire déconnecter le processus A du processus B). Il est important de tester une cyberposition défendable avant l'exécution, peut-être par un exercice de gestion des incidents dans le cadre d'un test planifié. Un sous-ensemble de la cyberposition défendable pourrait conduire à des opérations manuelles, sans l'aide d'interfaces humain-machine autonomes basées sur Windows, mais plutôt en travaillant à partir d'interfaces humain-machine intégrées, tels que ceux incorporés dans les équipements du SCI par l'intermédiaire des panneaux sur les appareils, ou en effectuant des opérations entièrement manuelles, avec des segments de réseau déconnectés pour isoler davantage les réseaux de SCI de l'usine.

Communications pendant l'intervention lors d'un incident

Lors d'un incident, une analyse ou une évaluation d'impact doit être présentée aux principaux intervenants dans le processus du SCI, avec la présence d'un personnel expérimenté en ingénierie des procédés. L'engagement des intervenants est essentiel pour assurer la coordination

et la faisabilité de l'intervention, si les recommandations en matière de sécurité doivent toucher ou modifier les opérations des SCI au fur et à mesure du déroulement des incidents. Cela permet à toutes les parties concernées d'avoir une compréhension claire de l'incident, et permet la communication nécessaire qui peut aider à assurer la sécurité de tous sur les sites.

Remarque : **le confinement** peut se faire en toute sécurité, mais **l'éradication** pourrait devoir attendre le prochain arrêt prévu des opérations. Si tel est le cas, une surveillance supplémentaire peut être nécessaire pour que la menace reste contenue.

Champ d'application et changements environnementaux

Le triage initial fournira idéalement des indicateurs de compromission. Il peut s'agir d'adresses IP de commande et de contrôle, de ports et de protocoles utilisés par la menace, ou de comportements de fichiers ou d'indicateurs et d'informations de processus qui peuvent à leur tour être utilisés pour une action défensive et préventive. Les indicateurs de compromission sont utilisés pour bloquer les opérations (voire les entraver), pour repérer les actifs et les réseaux potentiellement touchés et pour déterminer les vecteurs de menace. Les indicateurs de compromission et tout comportement identifié à partir de l'analyse de triage doivent être utilisés directement pour appliquer des contre-mesures sur tous les paliers de cybersécurité applicables. Ces contre-mesures pourraient inclure le blocage des ports sur les commutateurs de l'usine, l'ajout de règles de pare-feu pour bloquer les indicateurs de compromission, la désactivation (c'est-à-dire le durcissement) des services qui ne sont pas utilisés actuellement, la segmentation logique des réseaux ou la déconnexion complète de l'accès à distance pendant une intervention lors d'incidents. Toutes les mesures prises doivent tenir compte de l'impact potentiel qu'elles auront sur l'exploitation et la sécurité des travailleurs du site et de l'usine.

Prendre la décision d'avoir une incidence sur les opérations

Les interruptions du fonctionnement du SCI ne doivent se produire que lorsqu'il existe une menace imminente pour le système, ou lorsqu'il existe une menace qui a une incidence sur la perte de contrôle, la perte de surveillance des opérations, l'interruption des opérations ou la capacité de manipuler les opérations. Les intervenants de l'établissement ou les principaux décideurs doivent toujours être présents dans la salle avant tout changement au processus du SCI du site. Considérez les changements logiques avant d'envisager les changements physiques. Par exemple, considérez des changements tels que la mise en œuvre de règles de pare-

feu supplémentaires, la désactivation du protocole d'accès à distance aux ordinateurs de bureau ou l'ajout de listes de contrôle d'accès plus strictes avant d'envisager de déconnecter des câbles physiques, à moins que l'équipement à déconnecter ou à changer ne fasse déjà partie de votre cyberposition défensive testée.

Étape 7 : Déterminer comment le PRIC s'intégrera dans un plan de gestion de crise

L'objectif principal de cette étape est de tirer parti de tout plan de gestion des situations d'urgence (PGSU) ou plan d'intervention d'urgence qui pourrait déjà exister au sein de votre organisation, et de le relier au PRIC commun en TI et en TO.

Comme indiqué précédemment dans le présent document, ces plans, s'ils existent, peuvent également constituer un bon point de départ pour le développement d'un PRIC commun en TI et en TO. En mettant en place des points d'intégration entre le PRIC, le PGSU de l'entreprise et le plan d'intervention d'urgence du site, l'organisation aura une meilleure capacité de réaction en cas d'incident.

Les éléments suivants doivent être pris en compte lors de l'examen du PGSU existant et du plan d'intervention d'urgence au sein d'une organisation :

1. Revoir les définitions de ce qui constitue une crise ou une situation d'urgence;
    - Intégrer de nouvelles définitions si les cyberincidents des TO ne sont pas déjà couverts de manière adéquate.
    - Modifier le contenu existant si un aspect de l'environnement des TO est manquant.
2. Revoir les rôles et les responsabilités dans le cadre du plan de gestion des crises;
    - Veiller à ce qu'il y ait un coordinateur de la lutte contre les cyberviolations des TO (atteinte à la cybersécurité) qui puisse assurer la liaison entre le PRIC et l'équipe de gestion de crise.
    - S'il existe un coordinateur de la lutte contre les cyberfraudes envers les TI, négocier les options dans le cadre du plan.
    - Ajouter de nouvelles responsabilités aux rôles existants afin de renforcer les capacités en cas d'incident cybernétique dans le cadre des TO.

3. Examiner comment le PGSU et le plan d'intervention d'urgence sont invoqués;
    - Mettre à jour le PRIC avec des informations sur la manière de faire passer un incident de cybersécurité concernant les TO au plan de gestion de crise.
    - Mettre à jour le PGSU et le plan d'intervention d'urgence de l'organisation, afin d'inclure un contexte sur ce à quoi il faut s'attendre lors d'une intervention en cas d'incident de cybersécurité touchant les TO.
4. Inclure les équipes de gestion de crise et d'intervention d'urgence dans toute mise à jour des plans, y compris les options :
    - Exercices sur table;
    - Réunions de formation.

Le PRIC devrait travailler en collaboration avec le PGSU ou le Plan de gestion de crise. Cela garantira que tous les partenaires internes et externes nécessaires sont correctement pris en compte et que leurs fonctions et responsabilités sont correctement couvertes. Selon le niveau de gravité de l'incident, un incident de cybersécurité peut être un type de crise ou une situation d'urgence. Même si le plan d'intervention de la cybersécurité en cas d'incident dispose de ses propres mesures correctives, de nombreux rôles et responsabilités au sein du PGSU sont nécessaires, comme la consultation du conseiller juridique et la consultation des relations publiques.

Il est possible qu'un scénario d'attaque de cybersécurité crée des conditions dangereuses dans une installation, ce qui pourrait provoquer une crise. Un PGSU doit disposer d'un processus permettant de fermer l'installation en toute sécurité si cela se produit. Pour y parvenir, des personnes ayant une connaissance spécifique des exigences de sécurité des installations devront répondre de manière appropriée aux incidents de cybersécurité de cette ampleur. L'équipe de gestion de crise est habilitée à prendre des décisions commerciales liées à l'impact de l'incident. Que le PRIC soit un document autonome ou qu'il fasse partie du PGSU, les deux doivent être conçus pour fonctionner ensemble de façon harmonieuse.

Maintenir le PRIC commun dans les TI et les TO

La mise en place d'un PRIC commun dans les TI et les TO n'est pas un exercice de type « le préparer et l'oublier ». Une fois qu'un plan est en place, il devra être maintenu à jour en permanence pour demeurer pertinent.

En supposant une double direction, comme c'est généralement le cas avec la direction des TI et des TO, les gardiens du plan d'intervention devraient résider dans les deux environnements et défendre le rôle de chacun. Pour y parvenir, l'approche suivante est recommandée :

- Organiser régulièrement des réunions d'examen des réponses aux incidents, afin de tenir les membres de l'équipe d'intervention informés des événements et incidents récents.
- Tenir la direction informée des réunions et de leurs résultats, et lui donner une idée de votre état de préparation. Communiquer les résultats des réunions aux experts en la matière.
- Si vous avez constitué une matrice d'équipe d'intervention composée d'experts de différents secteurs de votre organisation et que les membres de cette équipe peuvent devenir actifs à tout moment, il sera important de faire une rotation lors de vos réunions hebdomadaires ou bihebdomadaires, afin de vous assurer qu'ils gardent une conscience de la situation des environnements qu'ils soutiennent.
- Soyez prêt à réaliser votre plan :
  - Vérifiez régulièrement la communication avec vos interlocuteurs, experts en la matière. Soyez créatif; vous pouvez avoir accès à toutes les ressources documentées de façon adéquate, mais il est possible qu'elles ne soient pas disponibles pour répondre, ou que leurs remplaçants désignés ne soient pas au courant de leurs disponibilités.
  - Organisez périodiquement des exercices autour d'une table pour valider les procédures et les communications (moins

fréquemment, mais sur une base régulière, afin de permettre une plus grande participation).
- Soyez prêt à former les nouveaux membres de l'organisation (si nécessaire).
- Après un exercice, assurez-vous que les conclusions pertinentes sont consignées dans un document sur les « leçons apprises » et que des mesures sont prises pour garantir que les faiblesses et les vulnérabilités soient résolues ou traitées. Une faille fatale dans un exercice permet de réapprendre les mêmes leçons lors d'un incident réel.

« Une faille fatale dans un exercice permet de réapprendre les mêmes leçons lors d'un incident réel. »

- Déléguez clairement le pouvoir de modifier le plan si nécessaire, et définir ce qui doit être communiqué et à qui, ainsi que le moment où cela doit se produire.
- Communiquez. Préparez des listes de contrôle. Faites la promotion du plan et informez les autres de sa localisation (avec des contrôles d'accès, bien sûr). Conservez une copie imprimée avec un accès contrôlé.

Conclusion

Cette directive a été créée dans le but de fournir aux organisations qui utilisent actuellement les TO la compréhension nécessaire de l'importance de mettre en œuvre un plan d'intervention en cas d'incident, qui peut mieux cibler les implications uniques qui ont une incidence sur les systèmes des TO. Cette ligne directrice, appliquée dans le contexte d'une organisation particulière qui est déjà équipée de fonctionnalités et de capacités informatiques, permettra une meilleure préparation et une meilleure défense contre les futurs menaces et incidents cybernétiques qui pourraient survenir dans les TI et les TO.

L'analyse des types de ressources des TO qui peuvent être vulnérables aux cybermenaces au sein d'une organisation permet de sensibiliser les organisations à l'importance de s'assurer que les systèmes de TO sont suffisamment protégés. Il offre également des informations et des lignes directrices importantes à prendre en compte qui doteront les équipes d'intervention en cas d'incidents de capacités suffisantes pour traiter et atténuer les risques associés aux cyberincidents liés aux TO. En fournissant une série de facteurs qu'une organisation doit prendre en compte en fonction de caractéristiques organisationnelles et de circonstances opérationnelles distinctes, les organisations peuvent être mieux préparées à de futurs incidents en TO liés à la cybernétique que les plans d'intervention en cas d'incident propre aux TI sont incapables de traiter de manière adéquate.

Glossaire

Agent principal de gestion du risque Ce cadre supérieur est chargé d'identifier, de gérer et d'atténuer les risques internes et externes auxquels l'organisation doit faire face.

Approche centralisée Un modèle de structuration des capacités d'intervention en cas d'incidents dans une organisation, en se basant sur la taille, la structure et les caractéristiques propres à cette organisation. Exige que l'EIIC consacre tout son temps et toutes ses ressources à l'intervention en cas d'incidents au sein de l'organisation.

Approche décentralisée Modèle de structuration des capacités d'intervention en cas d'incidents au sein d'une organisation, basée sur la taille, la structure et les caractéristiques propres à cette organisation. Permet aux intervenants d'avoir des rôles en dehors de l'EIIC, où ils ne sont appelés à intervenir qu'en cas d'incident.

Centre des opérations de sécurité Une unité centralisée au sein d'une organisation qui s'occupe des questions techniques et de sécurité.

C-I-D Triade Les trois composantes associées à la sécurité des réseaux. Exige que les systèmes de réseau comprennent des éléments de confidentialité, d'intégrité et de disponibilité.

Contrôleur de logique programmable Dispositif informatique spécialisé, utilisé pour les SCI, généralement utilisé pour l'automatisation des processus électrochimiques industriels dans le contrôle des machines.

Dirigeant principal de l'information Le cadre supérieur chargé de gérer et de superviser la stratégie en matière de TI et les autres systèmes informatiques utilisés et sur lesquels s'appuie une organisation.

Dirigeant principal de la sécurité Le cadre supérieur responsable de la sécurité physique d'une organisation, qui supervise la protection de son personnel, de ses biens, de son infrastructure et de sa technologie.

Équipe de gestion des situations urgence Les groupes élus d'une organisation, chargés de superviser le plan de gestion de crise et d'atténuer les risques associés aux menaces et incidents cybernétiques.

Équipe de la haute direction Une équipe de dirigeants d'une organisation, y compris les plus hauts niveaux de gestion, qui sont responsables de la gestion et de la supervision des opérations.

Équipe d'intervention en cas des incidents Une équipe d'intervention en cas d'incidents est un groupe de personnes (soit du personnel informatique avec une certaine formation en sécurité, soit du personnel de sécurité à plein temps dans les grandes organisations) qui collecte, analyse et agit en fonction des informations concernant un incident.

Équipe d'intervention en cas des incidents cybernétiques (EIIC) Une équipe d'intervenants spécialisés dans les incidents, chargée de traiter et d'atténuer les cyberincidents dans les TI et les TO, lorsqu'ils surviennent au sein d'une organisation.

Indicateurs de compromission Signatures d'ordinateurs qui identifient une activité potentiellement malveillante dans un système ou un réseau.

Interface humain-machine (IHM) Fournir une vue textuelle ou graphique d'un système et de ses opérations, permettant une surveillance, un contrôle, un rapport d'état et d'autres fonctions.

Network Mapper (NMAP) Un balayeur de réseau gratuit à code source ouvert, utilisé pour découvrir les hôtes et les services d'un réseau informatique en envoyant des paquets et en analysant les réponses.

Outil d'évaluation de la cybersécurité Un produit développé par le Department of Homeland Security des États-Unis qui aide les organisations à protéger leurs cyberactifs.

Plan de gestion de situation d'urgence (PGSU) Un processus prédéfini qu'une organisation suit lorsqu'elle traite une crise ou un incident.

Plan de réponse aux incidents cybernétiques (PRIC) Processus prédéfini auquel une organisation se réfère pendant et avant les cyberincidents qui menacent les systèmes ou ressources technologiques utilisés par l'organisation.

Plan d'intervention d'urgence Un processus prédéfini auquel une organisation se conforme en cas d'urgence. Comprend les actions, les ressources, les procédures et les protocoles nécessaires.

Plan d'intervention en cas d'incident (IRP) Un plan qui aide les organisations à se préparer et à prévenir les incidents de sécurité.

Protocole de bureau à distance (RDP) Protocole conçu pour faciliter le contrôle à distance des hôtes d'un réseau.

Réseau privé virtuel (RPV) Un réseau privé qui protège votre vie privée et préserve votre anonymat en ligne, en créant un réseau privé à partir d'une connexion Internet publique. Ce réseau masque votre adresse de

protocole Internet afin que vos agissements en ligne soient pratiquement impossibles à retracer. Plus important encore, les services d'un réseau privé virtuel établissent des connexions sécurisées et cryptées pour assurer un niveau de confidentialité que même un point d'accès Wi-Fi sécurisé ne peut atteindre.

Service téléphonique ordinaire Un service téléphonique standard et de base qui offre une connexion au réseau téléphonique pour de nombreuses résidences et petites entreprises dans le monde entier.

Système de contrôle de surveillance et d'acquisition de données (SCADA) Ensemble d'ordinateurs, d'interfaces, de systèmes et de configurations de réseau multiples utilisés pour régir et contrôler un environnement ou une installation de SCI.

Système de contrôle des turbines (TCS) Des systèmes de contrôle uniques conçus pour le contrôle des turbines.

Système de contrôle distribué (DCS) Système qui utilisent plusieurs contrôleurs, ordinateurs et capteurs à travers une infrastructure ou une usine pour faciliter le contrôle.

Système de contrôle industriel (SCI) Systèmes de contrôle associés à l'instrumentation utilisée pour le contrôle des processus industriels. Inclus les dispositifs, systèmes, réseaux et contrôles utilisés pour faire fonctionner ou automatiser les processus industriels.

Système de sécurité instrumenté (SIS) Système chargé d'assurer la sécurité d'une usine ou d'une organisation qui perçoit les conditions à risque qui se produisent et agit en conséquence pour éviter les accidents à l'intérieur et à l'extérieur de l'installation.

Technologie de l'information (TI) L'utilisation de matériel et de logiciels pour maintenir et résoudre des réseaux d'entreprise et des systèmes informatiques.

Technologie opérationnelle (TO) L'utilisation de matériel et de logiciels conçus pour gérer, surveiller et contrôler les opérations et les actifs industriels.

Très haute fréquence (VHF) Fréquence radio couramment utilisée, plus adaptée aux environnements extérieurs, souvent utilisée pour les professions de plein air comme la sylviculture et le pétrole.

Ultra Haute Fréquence (UHF) Fréquence radio couramment utilisée, plus adaptée aux environnements intérieurs, souvent utilisée par les écoles, les entrepôts et les magasins de détail.