Global Material Security

La amenaza interna

Dr. Justin R. Kinney
Colaborador de I+D, Laboratorio Nacional de Oak Ridge
Administración Nacional de Seguridad Nuclear
Departamento de Energía de EE. UU.

National Nuclear Security Administration

U.S. DEPARTMENT OF ENERGY

Definiciones

Global Material Security

- Agente interno: Son personas “con acceso autorizado a materiales nucleares [u otros materiales radiactivos], las instalaciones conexas o actividades conexas, o a la información de carácter estratégico o los recursos de información de carácter estratégico” (Guía No. 8-G Rev. 1 del OIEA)
- Los agentes que representan una amenaza interna pueden usar su **acceso, conocimientos** o **autoridad** para explotar, anular o eludir los sistemas de seguridad e intentar una retirada no autorizada o actos de sabotaje. Con ello, pasarían de ser una posible amenaza a convertirse en un adversario.
- Importante: acceso **legítimo y autorizado** a zonas controladas
  - Esta lista incluye empleados, exempleados, contratistas y consultores, proveedores, reguladores e inspectores, primeros actuantes o incluso visitantes de un sitio

Definiciones, continuación…

Global Material Security

Acceso: Persona autorizada y capaz de eludir las medidas de seguridad en zonas restringidas. Eso abarca el acceso físico, acceso a los sistemas informáticos (incluso podría ser acceso remoto). Ofrece oportunidades

Autoridad: Persona con la potestad o el derecho a realizar operaciones, girar instrucciones a empleados, exigir la obediencia de otros o utilizar equipos y tareas

Conocimientos: Posibles blancos de robo o sabotaje; planos de distribución de las instalaciones; cómo adquirir o utilizar herramientas y equipos, sistemas y medidas de seguridad física

(No necesariamente precisa de los tres elementos para cometer un acto doloso)

Extremismo

Global Material Security

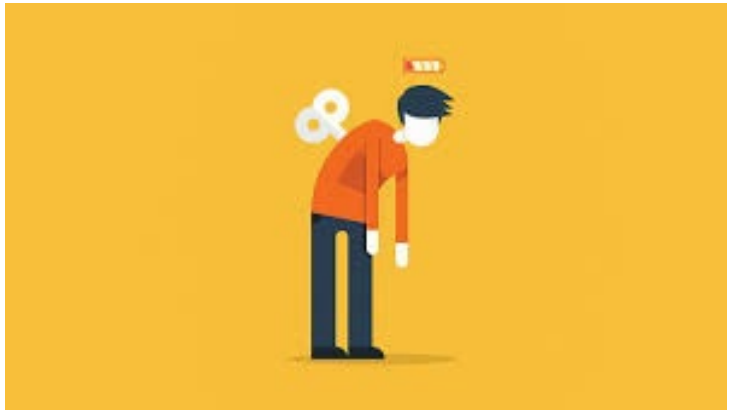
- Muchas motivaciones o vías psicológicas
  - Miedo, soledad, percepción de falta de oportunidades, sentirse víctima

- Procesos de radicalización:
  - Razonamiento emocional (amplificación de la ira o el miedo)
  - Determinación del blanco (direccionar el odio)
  - Polarización (mentalidad de nosotros contra los demás)
  - Separación y aislamiento de los 'no creyentes' (a menudo amigos y familia)
  - Grupo de apoyo social
  - Sentirse dueños de la verdad - moralidad, 'derechos'

Tipos de amenazas de agentes internos: Involuntario

Global Material Security

- (A veces llamados marionetas o peones)
  - Sin intención; accidental
  - Sin hostilidad ni mala voluntad
  - Deficiencia de capacitación
  - Ignorancia, falta de atención, distracción o negligencia
  - Posiblemente debido a enfermedad o fatiga
  - Imprudencia
  - Podría ser tan sencillo como pulsar un enlace malicioso en un correo electrónico o no verificar una alerta porque últimamente ha habido falsas alarmas
  - A menudo un adversario los usa como instrumentos o peones



Tipos de amenazas de agentes internos: Malintencionado

Global Material Security

- (A veces llamados chaqueteros o camaleones)
  - Acto intencional, deliberado, con conocimiento
  - Intenta causar daño; es hostil
  - Robo de materiales, información o propiedad intelectual
  - Sabotaje de materiales o sistemas
  - Podría ser un lobo solitario
  - Podría ser un colaborador (confabulado con una amenaza u organización externa)
    - Reclutado por un adversario que pretende aprovecharse del acceso, la autoridad o los conocimientos de un agente interno
    - O se ve obligado a hacerlo mediante coacción

Motivaciones del agente interno o detonantes para actuar con dolo

Global Material Security

- Convicción ideológica: radical o extremista; religiosa o secular; por etnia o nacionalidad; ambiental. Lealtades divididas
- Motivos financieros: motivado por el dinero; podría estar pasando un momento de dificultad debido a gastos médicos u otras obligaciones financieras
- Ego: arrogancia; probar sus propias habilidades; narcisista
- Psicótico: enfermedad mental; funcional y capaz, pero existe una inestabilidad subyacente
- Venganza: empleado (exempleado) o cliente descontento; pretende vengarse de la organización por lo que percibe como un desaire (no considerado para un ascenso; evaluación negativa)
- Coacción: amenazas de un adversario, ya sea a la persona, a su familia o a otros seres queridos. Podría ser daño físico, a la reputación u otros.

Agentes internos pasivos o activos

Global Material Security

- Pasivo
  - No dispuesto a cometer un acto de violencia ni lastimar a otros
  - Por lo general, entrega información básica para ayudar a los adversarios **externos** a obtener acceso o realizar un acto doloso
  - Por ejemplo, no cerrar con llave una puerta; dejar una computadora conectada y desatendida; revelar una contraseña
- Activo
  - Por lo general, tampoco es violento, pero *puede* volverse violento, dependiendo de las circunstancias
  - Entrega información, pero también está dispuesto a realizar acciones
    - Abrir puertas, manipular equipos, involucrar al personal de respuesta
    - Cuanto más activa es la amenaza, menos probable es que le preocupe que le atrapen o que tema perder su trabajo, etc.

Estudio de caso: Glenn Michael Souther

- Fotógrafo de la Marina, luego reservista en una instalación segura que procesa fotos de reconocimiento satelital
- Desertó a la URSS en 1986
  - Reveló información y fotos sobre armas, movimientos, criterios para un ataque nuclear
- Motivaciones: Desilusión con su trabajo, ideología, dinero
- Reclutamiento: Se ofreció para trabajar con los servicios soviéticos de inteligencia
- Acceso a la información: A través de sus tareas normales y se aprovechó de una laxa seguridad
- Los colegas no denunciaron múltiples indicadores: Horas de trabajo inusuales; riqueza injustificada; viajes sospechosos al extranjero, etc.
- Fallo en la verificación de antecedentes
  - Las denuncias de la exesposa sobre su inestabilidad y deserción fueron desestimadas

Estudios de casos de amenazas internas radiológicas y nucleares

Global Material Security

Quién	Cuándo	Dónde	Cómo	Por qué	Recomendación para la mitigación
Pirata informático (*hacker*) envió un correo electrónico a investigadores, haciéndose pasar por un estudiante	De noviembre 2015 a junio 2016	Centro de Investigación de Isótopos de Hidrógeno de la Universidad de Toyama, Japón	Un archivo malicioso adjunto en el correo electrónico fue abierto accidentalmente, dando acceso a información y datos personales	Agentes internos – Involuntarios Pirata informático -- Desconocido	Capacitación en ciberseguridad Configuración de correo electrónico y software antiphishing
Dos agentes internos: antiguo Director Administrativo y un chofer	Abril 2014	Planta de Sogetrap en Argelia	Un equipo de dos agentes internos robó un densímetro de rayos gamma con una fuente radiactiva	Sin especificar	Políticas de desvinculación: - Revocación del acceso a exempleados - Seguridad física para que el dispositivo sea menos portátil
Cuatro empleados y cuatro personas externas	Febrero de 2017	Empresa de exploración petrolífera y de gas de Malasia	Dos proyectores gamma con iridio-192 fueron sustraídos utilizando una furgoneta de la empresa	Ganancias económicas	Normas sobre el almacenamiento de vehículos Seguridad física mejorada

Evaluación de amenazas: Blancos

Global Material Security

- Blancos de robo o sabotaje
  - Materiales radiactivos o nucleares
  - Edificios o equipos
  - Componentes o sistemas
  - Procesos de transporte
- Información
  - Sobre las instalaciones, los empleados, información personal o sobre el trabajo que se realiza allí
- Propiedad intelectual
  - Patentes, planes, etc.

Ejercicio de reflexión

Global Material Security

¿Cómo podría una amenaza interna con intenciones dolosas obtener información sobre una expedición de material radiactivo y utilizar ese conocimiento para realizar un ataque?

Los horarios de transporte se encuentran entre los más vulnerables en cualquier situación, pero sobre todo los horarios de artículos de gran valor y alta peligrosidad, como los materiales radiactivos o nucleares.

Saber cómo, cuándo y dónde se mueve este material podría ser información muy útil para una amenaza interna

¿Cuáles son las señales? Indicadores de comportamiento

Global Material Security

- Expresa inconformidad con las políticas
  - Desacuerdo con políticas corporativas, de gerencia y federales
- Absentismo
- Altercados fuertes y hostiles con compañeros de trabajo
- Matonismo o comportamiento manipulador
- Adicciones
  - por ejemplo al alcohol, drogas
- Dificultades económicas
  - Problemas personales o familiares
- Exagerado interés en proyectos fuera de su alcance

Reconocimiento: ¿Cuáles son las primeras señales de alerta?

Global Material Security

- Indicadores virtuales o informáticos
  - Cambios en el horario habitual de trabajo
    - En línea a horas inusuales
  - Accede a datos a los que normalmente no accede
    - Horarios, lugares, etc.
  - Descarga grandes cantidades de datos
    - Particularmente si tienen muy poco motivo para trabajar con esos datos
  - Acceso no autorizado a dispositivos de almacenamiento

    (por ejemplo, memorias USB)

Reacción: Medidas preventivas

Global Material Security

Se utilizan para reducir la cantidad de agentes internos o para minimizar las oportunidades

- Verificación de la identidad
  - Control de acceso y escaneos de identidad en varios niveles
- Evaluación de probidad
  - Revisión de antecedentes (monitoreo inicial Y continuo); verificación de la identidad
  - Comprobación antes de otorgar autorizaciones; evaluaciones de confiabilidad
    - Riesgo de terceros proveedores que quizá no tengan los mismos controles
- Escolta y vigilancia
  - Cámaras con monitoreo activo, personal múltiple
  - Regla de la actuación por pareja, para evitar que los empleados accedan solos a las zonas seguras. Esto abarca tanto prevención como protección
- Concienciación en materia de seguridad física
  - Mejor y mayor capacitación: seguridad física y cibernética

Más medidas preventivas

- Confidencialidad
  - Diferentes niveles de acceso
- Garantía de calidad
  - Vigilancia
- Satisfacción de los empleados
  - Entornos de trabajo positivos
  - Los empleados deben sentirse valorados, respetados y escuchados
- Compartimentación (de datos, actividades y áreas físicas)
- Separación de tareas
  - Evita que una sola persona sepa demasiado
- Sanciones
  - En caso de infracciones

Niveles de monitoreo

Global Material Security

- Monitoreo de la empresa
  - Alarmas, inspecciones periódicas, configuración y software antiphishing
  - Personal de seguimiento
    - Tarjetas de identificación, puestos de control, etc.
  - Comprobación de antecedentes y autorizaciones de seguridad
    - Trastornos del comportamiento, enfermedad mental, antecedentes penales, problemas económicos, problemas familiares

- Monitoreo de los empleados
  - Reconocimiento entre pares de comportamientos anormales o dañinos
  - Los compañeros de trabajo están en la mejor posición para notar un comportamiento aberrante o conocer las dificultades personales de los demás
    - Entonces, pídales ayuda: Capacítelos para reconocer las señales y tener la capacidad y posibilidad de reaccionar o denunciar, según corresponda a su función
    - A veces solo se necesita que una persona se dé cuenta que un compañero de trabajo tiene dificultades y sea un buen amigo

Medidas de protección

Global Material Security

- META: Detectar, demorar, mitigar, revertir la amenaza
- Detener la adquisición (robo) o el sabotaje de materiales, o al menos retardarlo para permitir que llegue el personal de respuesta
  - Cerraduras, múltiples niveles de seguridad, barreras que requieran herramientas y habilidades especiales o personal adicional, etc.
  - Demorar hasta que el personal de seguridad pueda responder
- Todos los empleados deben recibir capacitación para reaccionar y enviar alertas de información, según sea necesario para sus funciones
  - Debemos empoderar a todos en la organización para ayudar a proteger las instalaciones y los materiales
  - Medidas de desescalada

Medidas de desescalada

- Relacionarse con la gente, hablar con ellos
  - Así sienten que estamos conscientes de su presencia
    - También construye una buena cultura de apoyo en la organización, la cual fortalece la cohesión
  - Comunicación
- Todos los empleados pueden aprender y capacitarse en técnicas de desescalada
- Es imprescindible crear relaciones sólidas y de confianza para gestionar mejor las amenazas. Los amigos, familiares y compañeros de trabajo cercanos son fundamentales para notar cambios preocupantes

Medidas de defensa en capas

Global Material Security

- Medidas técnicas
  - Sensores y alarmas
  - Monitoreo por circuito cerrado (CCTV)
  - Cerraduras y barreras en varios niveles
  - Sistemas de notificación
- Medidas administrativas
  - Verificación y capacitación
  - Conciencia del entorno (empoderar a todos los empleados en esta capacidad)
  - Observación y denuncias
    - Ofrezca vías seguras y razonables para que los empleados denuncien de forma anónima cualquier cosa sospechosa que vean

Etapas de la prevención y la protección

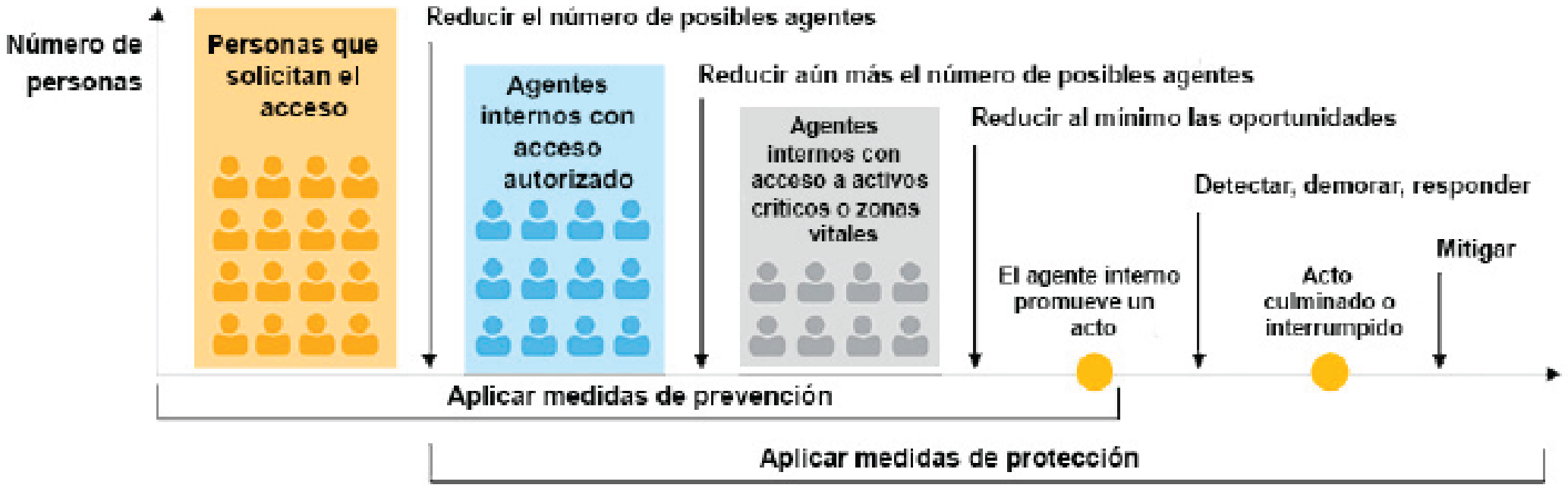


Fig. 1. Pasos en la utilización de las medidas de prevención y de protección frente a posibles amenazas de agentes internos.

Colección de Seguridad Física Nuclear del OIEA No. 8-G (Rev. 1): Medidas de prevención y de protección contra las amenazas de agentes internos

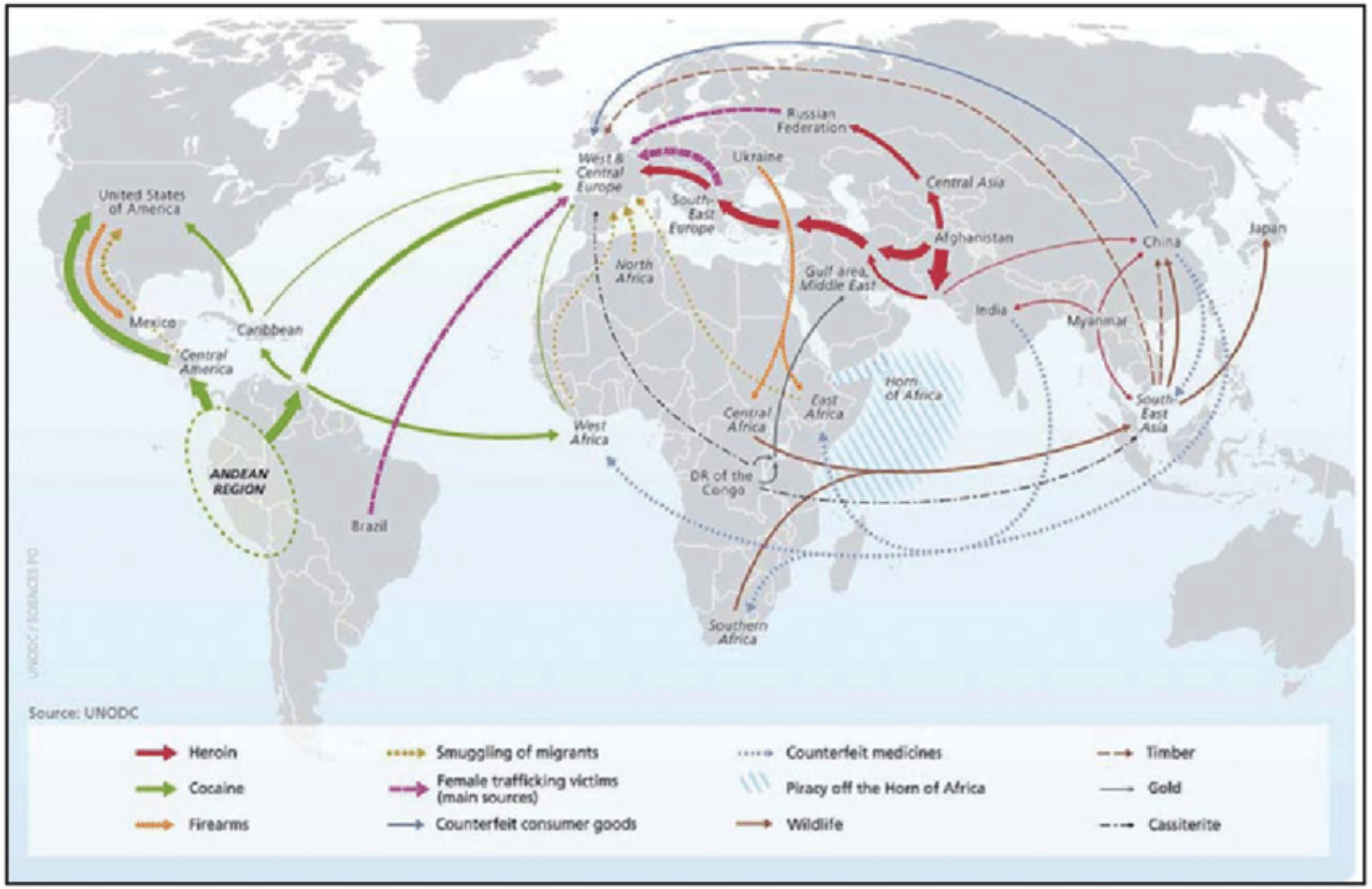
Amenaza secundaria: Crimen organizado transnacional

Global Material Security

- Grupos delictivos internacionales que trafican drogas, seres humanos y otros artículos ilícitos
- Sistemas establecidos para comprar y vender productos
- Debido a que han establecido rutas que saben que funcionan, otras organizaciones delictivas las usan para traficar sus propias mercancías
  - Drogas, seres humanos, mercado negro, etc.
- EJERCICIO DE REFLEXIÓN: ¿Qué sucedería si el crimen organizado transnacional y los grupos extremistas trabajaran juntos?
  - ¿Cómo podrían utilizar un agente interno en un caso como este?
  - Robo de artículos valiéndose de la condición del agente interno; vendidos en el mercado negro a través de la cadena de la organización delictiva

Rutas de contrabando establecidas por el crimen organizado transnacional

Global Material Security



Soluciones y resumen

Global Material Security

- IMPORTANTE: No existe una solución única para todas las amenazas internas
- Desafortunadamente, no hay una motivación sencilla que lo explique todo, ni un indicador universal del problema potencial, tampoco una respuesta única que funcione en todos los casos
- Cada instancia se refiere a una instalación, un entorno y a los empleados específicos que trabajan allí
- Sin embargo, existen medidas de prevención, protección, mitigación y respuesta que pueden emplearse para minimizar el riesgo en diferentes etapas
  - Técnicas o administrativas
  - Disuasión o detección o respuesta

Preguntas y comentarios

Global Material Security