Enhancing Office Security – Spanish



Muchos de nosotros vivimos con una falsa sensación de seguridad. Pensamos que el crimen les sucede a otras personas y que el terrorismo sucede en otros países. Desafortunadamente, eso no es cierto. Los asesinatos ocurren cada 21 minutos y los asaltos cada 16 segundos. Esto es especialmente cierto en el lugar de trabajo. Los edificios de oficinas en particular son lugares comunes para ataques criminales de todo tipo: por trabajadores descontentos, por perpetradores y víctimas de violencia doméstica e incluso por transeúntes con problemas mentales que buscan un lugar para vivir.

"La seguridad es una ilusión. La vida es una aventura atrevida, o no es nada en absoluto."

-Helen Keller.

La realidad es que debemos considerar todo tipo de amenaza a nuestra seguridad personal, incluso en el lugar de trabajo. Hablemos de las formas de entrenar a los trabajadores de oficina para que presten atención a la seguridad.

Desarmar las amenazas con una planificación proactiva

El arma más grande de un atacante es el elemento sorpresa. Actuar de forma reactiva es estar a la merced del atacante. Eliminar la sorpresa requiere un comportamiento proactivo. Como gerentes de seguridad, deben asumir la responsabilidad de la seguridad del lugar de trabajo. La seguridad de las instalaciones es típicamente el trabajo del oficial de seguridad interna; pero no pueden estar en todas partes a la vez. Aquí hay algunas pautas que le ayudarán a eliminar los riesgos comunes y a mejorar la seguridad de su oficina o de otro lugar de trabajo:

- Ponga barreras de acceso. Limite el acceso a sus instalaciones a los empleados y visitantes autorizados. Para mantener a todos los demás fuera, haga cumplir las prohibiciones de estacionamiento. Los atacantes a menudo conducen su vehículo directamente al edificio donde cometen sus ataques. Para reducir este riesgo, coloque divisores de concreto en las carreteras a lo largo del perímetro de sus instalaciones. Incluso puede usar barreras estéticamente agradables, como macetas, bancos de hormigón o esculturas.
- Retire los contenedores de basura. Retire los barriles de basura y los contenedores de residuos en las áreas comunes cerca de las entradas, tanto en el interior como en el exterior, donde los intrusos puedan tener acceso. Las oficinas ubicadas cerca de vecindarios residenciales podrían encontrar sus cubos de basura sobrecargados con desechos del propietario que podrían ser peligrosos o incluso explosivos.

- Asegure los respiraderos de la planta baja. Las rejillas de entrada de aire fresco a nivel de la calle están diseñadas para extraer aire para los sistemas de calefacción y refrigeración. Pero estos respiraderos plantean riesgos de bioterrorismo. Proteja su suministro de aire del sabotaje cercando las rejillas de ventilación en movimiento o moviéndolas a niveles más altos. Asegúrese de que el aire interior y exterior pase a través de filtros HEPA que eliminan todas las partículas de más de 1 micrón. También debe actualizar su sistema de detección de humo para aprovechar la nueva tecnología. Algunos detectores de humo ahora pueden detectar monóxido de carbono e incluso gas lacrimógeno, spray de pimienta y algunos gases nerviosos y armas químicas.
- Reduzca los puntos de entrada. Un único punto de entrada, siempre que sea posible, es lo mejor. Ayude al personal de seguridad a controlar quién entra en el edificio. También debería considerar la posibilidad de contratar a guardias entrenados para identificar posibles amenazas, en lugar de alguien que sólo comprueba las identificaciones. Los pedazos de papel con palabras y fotos laminadas en plástico son fáciles de falsificar.
- Instale cámaras de seguridad. Una cámara de seguridad es su ojo en el cielo. También necesita personas calificadas para “monitorear el monitor”. Pero recuerde que un solo guardia de seguridad viendo 50 pantallas de video no lo controlará. En grandes instalaciones, el guardia debe ser apoyado por guardias entrenados y motivados, dentro y fuera de la instalación, vigilando cada aspecto de su sitio en todo momento.
- Monitoreé el envío y la recepción. Este es un punto débil en la mayoría de los planes de seguridad a través del cual los intrusos pueden entrar. En el área de envío y recepción, el personal de seguridad debe:
    - Asegurarse de que nadie entre en el edificio; y
    - Revise y escanee todos los elementos antes de que entren en el edificio.
- Supervisar el uso de la web. Los empleados acceden a Internet en el trabajo tanto para actividades laborales como personales. También pueden usarla para actividades ilegales. De manera alarmante, el número de empleados que transmiten datos sensibles y de propiedad de la empresa a través de Internet está aumentando. Si esto es una preocupación en su organización, existen varias tecnologías de vigilancia que pueden ayudar a su departamento de IT a monitorear la actividad en línea. Muchas empresas utilizan estas técnicas para proteger sus inversiones.

Conclusión

Independientemente de las tecnologías y los métodos de seguridad que utilice, también debe pedir a un tercero que realice una auditoría de seguridad de sus instalaciones. Un profesional imparcial puede detectar las lagunas de seguridad y las vulnerabilidades exclusivas de su sitio y hacer recomendaciones para ayudar a asegurar el futuro de su lugar de trabajo, sus empleados y su negocio.