



Ataques cibernéticos en el Sector de Construcción

Dentro del sector de construcción, las empresas colaboran en un entorno digital. Muchas partes interesadas en los proyectos, desde contratistas y subcontratistas hasta arquitectos, ingenieros y topógrafos, tienen acceso a plataformas de TI compartidas de una forma única para la industria de construcción. Esta dependencia de redes, aplicaciones de software y datos compartidos proporciona una conectividad totalmente automatizada, lo que permite la comunicación y acceso a datos compartidos de maneras que no se imaginaban hace una década.

Este incremento en la eficiencia da como resultado un aumento en el riesgo, particularmente en un contexto de características específicas en el sector de construcción. Por un lado, el gran volumen de datos confidenciales compartidos (incluidos presupuestos, licitaciones, planos técnicos y diseño de productos, detalles comerciales o secretos industriales) conlleva riesgos de seguridad adicionales.

Otras características del sector incluyen el uso de tabletas, teléfonos inteligentes o computadoras portátiles (aumentando los puntos de vulnerabilidad del sistema) y la gran dependencia de subcontratistas y mano de obra transitoria, con la consiguiente presión en torno a la capacitación.

La construcción es un negocio con gran liquidez. El éxito de una empresa depende de su capacidad para cumplir con los plazos de los proyectos y las especificaciones del contrato, y para financiar a sus contratistas. Ciertos incidentes cibernéticos tienen el potencial de afectar la capacidad de una empresa para cumplir con estos objetivos.

¿Estamos realmente en riesgo?

Exposición de información corporativa confidencial

La exposición de información confidencial podría dar lugar a los siguientes costos directos y daños a terceros:

- Daños asociados con la liberación inadvertida de secretos comerciales.

- Reclamaciones de clientes y otros por el costo de rediseñar o reconstruir instalaciones o sistemas seguros.
- Investigación forense del incidente cibernético.
- Asesoramiento legal y costos de relaciones públicas sobre cómo responder.
- Gastos de defensa asociados a reclamaciones de terceros.
- Requisitos regulatorios. Si bien las multas pueden quedar cubiertas por una póliza de seguro siempre y cuando sean asegurables por ley, los costos de respuesta a una solicitud regulatoria generalmente están cubiertos por una póliza de seguro de cyber.

Violación de la seguridad de la red

- Problemas potenciales de seguridad con edificios y ciudades con tecnología innovadora, agravados por el aumento de las vulnerabilidades de IoT (Internet of Things).
- Pérdida de ingresos relacionada con la incapacidad de realizar negocios y proporcionar servicios (debido a la interrupción del negocio, problemas de flujo de efectivo, entre otras cosas).
- Daños sufridos por terceros que interactúan con el sistema de una empresa constructora.
- Pérdida de confianza por parte de los clientes y posible daño a la reputación.

Modelaje de Información para la Construcción

Modelaje de información para la construcción es un registro central que permite la entrada de varias partes, ya sea que trabajen de forma independiente para consolidar la información (nivel 2) o trabajando en el mismo modelo integrado al mismo tiempo (nivel 3). Debido a la naturaleza compartida del modelaje de información para la construcción y las numerosas partes interconectadas, los riesgos de una violación a la seguridad de datos son mucho mayores, particularmente dentro del nivel 3 de modelaje.

Las amenazas incluyen ganancias comerciales por medios delictivos mediante la explotación de la propiedad intelectual, el sabotaje del proyecto o el secuestro de información comercialmente sensible para pedir un rescate. La vulneración de una plataforma BIM alojada en una empresa de construcción puede tener implicaciones de responsabilidad derivadas de exposiciones contractuales a terceros.



Cobertura de Responsabilidad Civil Profesional

¿Cómo interactúa una póliza de seguro de cyber y complementa el seguro de Responsabilidad Civil Profesional (E&O/PI) de una empresa de construcción?

Cobertura bajo una póliza de Responsabilidad Civil Profesional (E&O/PI)

- Una pérdida cibernética, si estuviera cubierta por la póliza de E&O, estaría sujeta al deducible que tendría que desembolsar el mismo asegurado que a menudo es muy alto para las empresas de construcción el cual representaría un gasto elevado.
- Una pérdida cibernética puede erosionar los límites de PI disponibles para reclamos en errores profesionales de

construcción. Esto afectaría la siniestralidad, indemnización y potencialmente la prima.

- Para activar la cobertura bajo la póliza de PI, es posible que tenga que haber un error u omisión en la realización de servicios profesionales. Sin embargo, una empresa de construcción podría ser responsable por las violaciones de datos o seguridad de la red, incluso en ausencia de un error u omisión. Además, el incidente no siempre estará relacionado con la prestación de servicios profesionales.

Cobertura bajo una póliza de Seguro de Cyber.

- Los costos directos (pérdidas propias), como los costos forenses de TI (para determinar el origen, alcance, extensión de la violación y actuar para contenerla), costos legales y costos de relaciones públicas generalmente no están cubiertos por una póliza de PI, por otro lado, bajo una póliza de seguro de cyber si se estarían cubriendo. Una de las principales ventajas de una póliza de cyber es el acceso 24/7 a los servicios de respuesta a incidentes cibernéticos. En esas primeras horas después de un incidente, el acceso inmediato al soporte de TI para determinar el alcance, la causa o la magnitud del incidente será vital para minimizar el tiempo de inactividad y el daño financiero. Las empresas en el sector de construcción operan con plazos y fechas de entrega muy ajustados; es crucial que se mitigue la interrupción del negocio y se mantenga la planificación para garantizar un impacto mínimo en los acuerdos contractuales.
- Las pólizas de seguro de cyber a menudo responderán a una violación independientemente que sea una conducta ilícita o esté relacionado con los servicios profesionales.
- El seguro de cyber ayuda a que la pérdida que se llegue a presentar no tenga tanto impacto lo cual se traduce a un beneficio en liquidez y ahorro en gastos que se tendrían que erosionar en caso de no contar con dicha cobertura.

Caso de estudio

Una empresa de construcción recibió un correo por parte de un supuesto subcontratista, el correo se veía confiable, sin embargo, no se percataron que en realidad era un delincuente cibernético suplantando la identidad de dicho subcontratista, el cual compartió un malware a través de un link, dando como resultado la invasión a todos los sistemas de gestión y accediendo a la información sensible de la compañía, bloqueando el acceso a diferentes plataformas que eran esenciales para la operación, por lo que se estaba tratando de un secuestro de datos y denegación de acceso al sistema operativo.

La compañía acudió a las autoridades pertinentes y contrató a una empresa para llevar a cabo la investigación y negociación; afortunadamente lograron recuperar los datos secuestrados y acceder a su sistema operativo.

Después de revisar el incidente, las aseguradoras concluyeron que existía cobertura bajo la póliza de cyber tanto para los honorarios erosionados y la interrupción de negocio.

Seguro de Cyber Específico

En Lockton, nos especializamos en programas de seguros grandes y complejos para empresas enfocadas el sector de construcción e ingeniería civil. Nuestros programas de seguro se adaptan a las necesidades del riesgo, lo que garantiza una cobertura adecuada para todas las partes en todas las líneas de cobertura. Esta experiencia en la industria nos da una excelente exposición a los hábitos de compra cibernética y las exposiciones que enfrenta el sector de la construcción.

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para su organización de construcción. Es vital proteger los sistemas de una empresa para permitirle resguardar sus actividades, clientes, reputación e ingresos.

Reconocer las vulnerabilidades particulares en todo el sector de la construcción es fundamental.

Un ataque cibernético puede tener ramificaciones de gran alcance. Comprender estos riesgos y mitigarlos de manera proactiva es clave. Nuestro equipo de expertos en riesgos cibernéticos trabajará con usted para crear una solución personalizada que proteja y asegure su trabajo exactamente donde lo necesite y garantice que los riesgos cibernéticos se integren en su proceso de gestión de riesgos. Reconstruir la confianza es vital.

La seguridad de su cliente está en sus manos. Coloque la seguridad de su negocio en las nuestras.

Para mayor información:



Ricardo Millán
Head ProFin México
ricardo.millan@lockton.com



Moisés García
ProFin México
moises.garciab@lockton.com